CENTRO DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO
Universidad Tecnológica de Pereira

Universidad Tecnológica de Pereira

# Guía de Implementación de los Protocolos Border Gateway Protocol (BGP) y Multiprotocol Label Switching (MPLS)

Ana María López Echeverry
Miller Ramírez Giraldo
Edward Fabián Penagos Granada

Editorial UTP

Colección Ensayos

**Ana María López Echeverry, (Roldanillo, Valle, Colombia, 1972).**
Magister en Ingeniería de la Universidad Pontificia Bolivariana de Medellín e Ingeniera Electricista de la Universidad Tecnológica de Pereira. Profesora asistente de la Facultad de Ingenierías Eléctrica, Electrónica, Física y Ciencias de la Computación de la Universidad Tecnológica de Pereira. Ha publicado artículos en revistas especializadas nacionales e internacionales en temas relacionados con las telecomunicaciones, protocolos de comunicación, criptografía y seguridad de la información. Pertenece al Grupo de Investigación Nyquist.

anamayi@utp.edu.co

**Miller Ramírez Giraldo, (Pereira, Risaralda, Colombia,1981).**
Magister en Ingeniería de Sistemas y Computación e Ingeniero de Sistemas y Computación de la Universidad Tecnológica de Pereira. Docente de cátedra auxiliar de la Universidad Tecnológica de Pereira. Ha publicado artículos en revistas especializadas nacionales en temas relacionados con las telecomunicaciones. Pertenece al Grupo de Investigación Nyquist.

miller@utp.edu.co

**Edward Fabián Penagos Granada, (Bogotá, Cundinamarca, Colombia, 1990).**
Magister en Ingeniería de Sistemas y Computación, e Ingeniero de Sistemas y Computación de la Universidad Tecnológica de Pereira. Ha publicado artículos en revistas especializadas nacionales en temáticas relacionadas con la criptografía y la seguridad de la información. Pertenece al Grupo de Investigación Nyquist.

Efpenagos@gmail.com

# Guía de implementación de los Protocolos Border Gateway Protocol (BGP) y Multiprotocol Label Switching (MPLS). Aproximación Práctica

**Ana María López Echeverry**
**Miller Ramírez Giraldo**
**Edward Fabián Penagos Granada**

Universidad Tecnológica de Pereira

Colección Estado del Arte para Todos
Centro De Innovación y Desarrollo Tecnológico (CIDT)
2018

López Echeverry, Ana María
Guía de implementación de los protocolos Border Gateway Protocol (BGP) y Multiprotocol Label Switching (MPLS). Aproximación práctica / Ana María López Echeverry, Miller Ramírez Giraldo y Edward Fabián Penagos Granada. – Pereira : Universidad Tecnológica de Pereira, 2018.
225 páginas. – (Colección Estado del arte para todos).

ISBN: 778-958-722-315-6

1. Redes de datos 2. Enrutamiento 3. Topología de sistemas autónomos 4. Procesamiento electrónico de datos 5. Internet

CDD 004.6


Primera edición
Universidad Tecnológica de Pereira
Pereira, Colombia

ISBN: 778-958-722-315-6

**Colección Estado del Arte para todos:**
"Guía de Implementación de los Protocolos Border Gateway Protocol (BGP) y Multiprotocol Label Switching (MPLS). Aproximación Práctica".

Esta publicación ha sido realizada por el Grupo de Investigación Nyquist, en el marco del Proyecto Plataforma de Emulación de Servicios Sobre Redes Inteligentes, en el marco del proyecto Centro de Innovación y Desarrollo Tecnológico CIDT en su I Fase de implementación (2014-2017), financiada con recursos provenientes del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías, en asocio con la Gobernación de Risaralda, la Universidad Tecnológica de Pereira, la Alcaldía de Pereira, la Universidad Católica de Pereira, Parquesoft Pereira e Incubar Eje Cafetero.

**Universidad Tecnológica de Pereira**
©Centro de Innovación y Desarrollo Tecnológico (CIDT)
Editorial Universidad Tecnológica de Pereira

**Coordinador editorial:**
Luis Miguel Vargas Valencia
luismvargas@utp.edu.co
Tel: 3137381
Edificio 9 Biblioteca central "Jorge Roa Martínez" 9/N1/110
Cra 27 No. 10-02 Los Álamos
Pereira, Colombia
www.utp.edu.co

**Montaje y producción:**
Universidad Tecnológica de Pereira
Centro de Recursos Informáticos y Educativos CRIE

**Impresión y acabados:**
Publiprint
Pereira

**SISTEMA GENERAL DE REGALÍAS**
Luis Fernando Mejía, Director General, Departamento Nacional de Planeación (DNP)
Mauricio Cárdenas Santamaría, Ministro, Ministerio de Hacienda y Crédito Público
Germán Arce Zapata, Ministro, Ministerio de Minas y Energía
César Ocampo Rodríguez, Director, Departamento Administrativo de Ciencia, Tecnología e Innovación (Colciencias)
Luis Fernando Gaviria Trujillo, Presidente, Órgano Colegiado de Administración y Decisión (OCAD) – Fondo de Ciencia, Tecnología e Innovación, Risaralda

**GOBERNACIÓN DE RISARALDA**
Sigifredo Salazar Osorio, Gobernador de Risaralda
Diana Yaneth Osorio Bernal, Secretaria de Desarrollo Económico y Competitividad
Adrián Cardona Alzate, Asesor Secretaria de Desarrollo Económico y Competitividad

**ALCALDÍA DE PEREIRA**
Juan Pablo Gallo Maya, Alcalde de Pereira
Daniel Perdomo Gamboa, Secretario de Educación
Claudia Patricia Velásquez Lopera, Secretaría de Planeación

**UNIVERSIDAD TECNOLÓGICA DE PEREIRA**
Luis Fernando Gaviria Trujillo, Rector
Martha Leonor Marulanda Ángel, Vicerrectora de Investigación, Extensión e Innovación
Francisco Uribe Gómez, Jefe Oficina de Planeación
Viviana Barney Palacín, Directora CIDT

**UNIVERSIDAD CATÓLICA DE PEREIRA**
Ptro. Jhon Fredy Franco Delgado, Rector
Maria Paulina Giraldo, Directora Proyección Sociala
Andrés Henao Rosero, Decano Facultad de Ciencias Económicas y Administrativas
Yaffa Nahir Ivette Gómez Barrera, Decana Facultad de Arquitectura y Diseño

**PARQUESOFT**
Johanna Loaiza Mesa, Directora Ejecutiva Parquesoft Risaralda
Alexander Cadavid Giraldo, Director Parquesoft Colombia

**INCUBAR EJE CAFETERO**
Carlos Alberto Guevara, Director Ejecutivo Incubar Eje Cafetero

# ÍNDICE GENERAL DE LABORATORIOS BGP Y MPLS

## PRIMERA PARTE LABORATORIO BGP

## SEGUNDA PARTE LABORATORIOS MPLS

# ÍNDICE DE FIGURAS



# ÍNDICE DE TABLAS

## SEGUNDA PARTE LABORATORIOS MPLS

# CAPÍTULO UNO

# 1. LABORATORIO N° 1 - INTRODUCCIÓN A BGP

## 1.1. INTRODUCCIÓN

En la parte introductoria del protocolo BGP (Border Gateway Protocol) se iniciarà un trabajo pràctico que permite la comunicación entre sistemas autónomos, permitiendo validar conocimientos teóricos adquiridos a través de cursos de formación relacionados con este protocolo de comunicación.

En esta actividad, tendrá que construir una red a partir de una topología específica, diseñar un espacio de direccionamiento y requerimientos de red proporcionados. Luego implementar la configuración básica de BGP sobre la red.

## 1.2. OBJETIVOS

Al completar esta práctica de laboratorio usted podrá:

- Comprender el funcionamiento básico de BGP sobre enrutadores Cisco.
- Anunciar redes locales mediante BGP.
- Redistribuir rutas al interior de BGP.
- Realizar la configuración básica de agregación de ruta de BGP.
- Monitorear el estado del proceso de enrutamiento, vecindades y estados de BGP.

## 1.3. DIAGRAMA DE LA TOPOLOGÍA

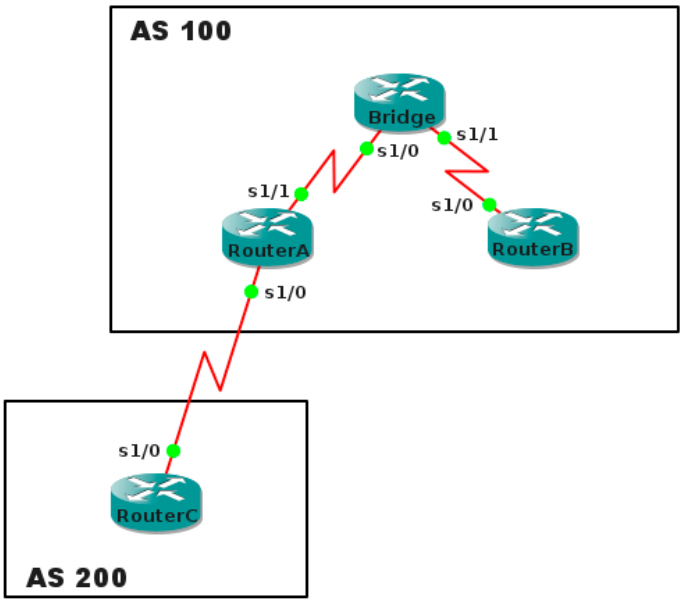


***Figura 1.1.*** Topología Introducción a BGP

## 1.4. TABLA DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| Router A | | | |
| | | | |
| | | | |
| Router B | | | |
| | | | |
| Router C | | | |
| | | | |
| Router Bridge | | | |
| | | | |

Tabla 1.1. Introducción a BGP

# 1.5. DESCRIPCIÓN DE LA ACTIVIDAD

## TAREA 1: División en subredes del espacio de direccionamiento

**Paso 1:** Examinar los requisitos de la red.

El direccionamiento para la red tiene los siguientes requisitos:

- Para el AS 100 ha sido asignado el espacio de direcciones 192.168.0.0/16, el cual debe dividirse en subredes para proporcionar direcciones a las LAN y enlaces seriales.
    - La LAN simulada por la interfaz Loopback del Router A requerirá 16.000 direcciones.
    - La LAN simulada por la interfaz Loopback del Router B requerirá 8.000 direcciones.
    - Los enlaces seriales entre los routers requerirán dos direcciones para cada enlace.

| **Dispositivo** | **Interfaz** | **No. de Subred** | **Dirección Subred** | **Máscara Subred** |
|---|---|---|---|---|
| Router A | Loopback 0 | 0 | | |
| Router B | Loopback 0 | 1 | | |

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| Router A <>Brigde | 0 | | |
| Router B <> Bridge | 1 | | |

- Para el AS 200 ha sido asignado el espacio de direcciones 172.16.0.0/16, el cual debe dividirse en subredes para proporcionar direcciones a la LAN.
    - La LAN simulada por la interfaz Loopback del Router C requerirá 25.000 direcciones.

| **Dispositivo** | **Interfaz** | **No. de Subred** | **Dirección Subred** | **Máscara Subred** |
|---|---|---|---|---|
| Router C | Loopback 0 | 0 | | |

- Para las conexiones externas entre los dos AS se ha asignado la red 10.1.0.0/30.

**Paso 2:** Documente el esquema de direccionamiento.

Documente las direcciones IP y máscaras de subred utilizando las tablas proporcionadas.

## TAREA 2: Preparación básica de la red

**Paso 1:** Conecte una red que sea similar a la del diagrama de topología.

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en el gráfico.

**Paso 2:** Configuración básica de los enrutadores.

Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautas generales (utilice como contraseña la palabra *"nyquist"*):

1. Configure el nombre de host del router.
2. Configure una contraseña de modo EXEC privilegiado.
3. Configure un mensaje del día.
4. Configure una contraseña para las conexiones de la consola.
5. Configure una contraseña para las conexiones de VTY.

## TAREA 3: Configurar y activar las interfaces

**Paso 1:** Configure las interfaces en los enrutadores con las direcciones IP de la tabla proporcionada debajo del Diagrama de topología.

## TAREA 4: Configuración del enrutamiento IGP

Consulte y analice:

¿Por qué es importante configurar un IGP antes de configurar BGP dentro de un AS?

_____

_____

_____

_____

Configure OSPF en cada uno de los enrutadores del AS 100 (utilice el Id de proceso 1 y el área 5 para las redes).

**Paso 1:** Configure OSPF en el Router A (Tenga en cuenta las redes que deben incluirse en las actualizaciones OSPF).

Es necesario redistribuir sobre OSPF las subredes de los enlaces directamente conectados al Router A, incluso aquellos que no participan en el intercambio de actualizaciones OSPF, tales como el enlace serial que comunica a los dos AS y la interfaz *Loopback*.

**Nota**: Tenga en cuenta que para las interfaces que **no** participan en el proceso de enrutamiento es necesario bloquear las actualizaciones OSPF con el uso del comando **passive-interface**.

**Paso 2:** Configure OSPF en el router Bridge (Tenga en cuenta las redes que deben incluirse en las actualizaciones OSPF).

**Paso 3:** Configure OSPF en el Router B (Tenga en cuenta las redes que deben incluirse en las actualizaciones OSPF).

Es necesario redistribuir sobre OSPF las subredes de los enlaces directamente conectados al Router B, incluso aquellos que no participan en el intercambio de actualizaciones OSPF, tales como la interfaz *Loopback*.

**Nota**: Tenga en cuenta que para las interfaces que **no** participan en el proceso de enrutamiento es necesario bloquear las actualizaciones OSPF con el uso del comando **passive-interface**.

## TAREA 5: Configuración del enrutamiento BGP

**Paso 1:** Inicie el proceso BGP en cada enrutador con el número AS específico (realizar el proceso de configuración en todos los enrutadores, tanto del AS 100 como del AS 200):

**router bgp** <*as-number*>

**Paso 2:** Establezca sesiones con pares BGP.

A diferencia de otros protocolos de enrutamiento, BGP carece de medios para establecer adyacencias (detectar vecinos) de forma automática. Cada router debe ser manualmente configurado con la información de cada vecino indicando a que direcciones IP dirigir sus intentos de conexión.[1]

El router que recibe los intentos de conexión compara la dirección IP de origen del paquete TCP SYN recibido, contra una lista de direcciones IP previamente configurada de posibles vecindades. Si el intento de conexión proviene de una de las direcciones de dicha lista, se establece la relación de vecinos, de lo contrario no se establece la adyacencia.[2]

**Nota:** El número de AS configurado determina si la sesión es una sesión EBGP (el AS vecino es diferente al AS local) o una sesión IBGP (mismo número de AS).

Dentro del AS 100 para cada enrutador es necesario establecer sesiones IBGP con cada uno de los otros enrutadores que se encuentran al interior del AS.

1 Cisco System Learning. Configuring BGP on Cisco Routers.Version 3.2. Volumen 1. Estados Unidos. 2005. p. 52

2 Ibíd., p. 52.

La sesión EBGP entre el AS 100 y el AS 200 sólo se debe establecer entre los enrutadores de borde, es decir, entre el Router A y el Router C.

Para establecer sesiones BGP entre router vecinos haga uso del comando de configuración:

**neighbor** <*neighbor-ip-address*> **remote-as** <*as-number*>

**Paso 3:** Habilite el proceso de autenticación entre las sesiones BGP.

Configure la autenticación de BGP utilizando el password "nyquist" mediante el comando:

**neighbor** <*neighbor-ip-address*> **password** <*authentication-password*>

**Paso 4:** Habilite la publicación de las subredes de las interfaces Loopback en los enrutadores que tienen configurada dicha interfaz.

Para esta tarea utilice el comando **network** para configurar manualmente la publicación de subredes.

**Paso 5:** Verificar configuración y conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos mediante el comando:

**show ip bgp summary**

Para realizar un ping a partir de una determinada dirección IP de una interfaz de router con destino a una dirección específica se utiliza el comando:

**ping** <*destination-ip-address*> **source** {<*source-ip-address*> | <*source-interface*>}

¿Es posible realizar un ping desde la LAN del Router A a la LAN del Router B? SI _____
¿Es posible realizar un ping desde la LAN del Router A a la LAN del Router C? SI _____

¿Es posible realizar un ping desde la LAN del Router B a la LAN del Router C? SI _____

¿Qué rutas BGP están presentes en la tabla de enrutamiento de Router A?

_____
_____
_____
_____

¿Qué rutas BGP están presentes en la tabla de enrutamiento de Router B?

¿Qué rutas BGP están presentes en la tabla de enrutamiento de Router C?

## TAREA 6: Habilitar la redistribución de rutas en BGP

**Paso 1:** Deshabilite la publicación de rutas manual en Router A y Router B.

Utilice la forma **no** del comando **network** para realizar esta TAREA (el comando network dentro del proceso de enrutamiento BGP).

**Paso 2:** Habilite la redistribución de redes directamente conectadas sobre el protocolo BGP.

La distribución de rutas directamente conectadas se debe realizar sobre el Router A, para lograr esta TAREA se utiliza el comando:

**redistribute connected**

Si se revisa la tabla BGP del Router A se podrá detectar que todas las redes que están directamente conectadas al Router A están disponibles para ser distribuidas hacia el Router C, sin embargo, se desea que sólo la red LAN simulada por la interfaz Loopback sea publicada.

**Paso 3:** Configuración de una lista de acceso para filtrado de rutas.

Configurar una lista de acceso en Router A que permita sólo la red que se desea distribuir y que rechace las demás redes.

Aplicar dicha lista de acceso en Router A para filtrar la distribución de redes hacia el Router C, mediante el comando:

**neighbor** <*neighbor-ip-address*> **distribute-list** <*access-list-number*> {**in** | **out**}

**Paso 4:** Habilite la redistribución de redes de un determinado IGP.

Habilite la redistribución de rutas del protocolo OSPF a través de BGP en el Router A, mediante el comando:

**redistribute** <*protocol*> [<*process-id*>] [**match** {**internal | external 1 | external 2**}]

**Paso 5:** Modificar la lista de acceso configurada para permitir la ruta redistribuida desde el IGP.

Se debe modificar la lista de acceso anteriormente configurada para añadir las redes redistribuidas desde OSPF dentro de BGP (redes Loopback de Router A y B), para que el Router A pueda publicarlas hacia el Router C.

Una vez que se haya modificado la lista de acceso, se debe reiniciar la sesión entre el Router A y el Router C mediante el comando (sólo es necesario realizarlo en uno de los dos enrutadores peer):

**clear ip bgp** <*neighbor-ip-address*>

**Paso 6:** Verificar las configuraciones y la conectividad.

¿Es posible realizar un ping desde la LAN del Router A a la LAN del Router B? SI _____
¿Es posible realizar un ping desde la LAN del Router A a la LAN del Router C? SI _____
¿Es posible realizar un ping desde la LAN del Router B a la LAN del Router C? SI _____

Mediante el comando:
**show ip bgp**

¿Qué rutas están presentes en la tabla BGP de Router A?

_____
_____
_____
_____

¿Qué rutas están presentes en la tabla BGP de Router B?

_____
_____
_____
_____

¿Qué rutas están presentes en la tabla BGP de Router C?

¿Qué rutas BGP están presentes en la tabla de enrutamiento de Router A?

¿Qué rutas BGP están presentes en la tabla de enrutamiento de Router B?

¿Qué rutas BGP están presentes en la tabla de enrutamiento de Router C?

## TAREA 7: Habilitar la sumarización de ruta de BGP

**Paso 1:** Habilite la sumarización de ruta de BGP en el Router A para el espacio de direcciones asignado al AS 100.

Utilice el comando de configuración de router:

**aggregate-address** <*network-ip-address*> <*network-mask*>
**Paso 2:** Verificar configuración y conectividad.

¿Es posible realizar un ping desde la LAN del RouterC a la LAN del RouterA? SI _____

¿Es posible realizar un ping desde la LAN del RouterC a la LAN del RouterB? SI _____

¿Qué rutas están presentes en la tabla BGP de RouterC?

¿Qué rutas BGP están presentes en la tabla de enrutamiento de RouterC?

_____
_____
_____
_____

**Paso 3:** Configure la sumarización de ruta de BGP para publicar sólo la red sumarizada.

Para publicar únicamente el resumen de ruta, se utiliza el comando:

**aggregate-address** <*network-ip-address*> <*network-mask*> **summary-only**

**Paso 4:** Verificar las configuraciones y la conectividad.

¿Es posible realizar un ping desde la LAN del Router C a la LAN del Router A? SI _____

¿Es posible realizar un ping desde la LAN del Router C a la LAN del Router B? SI _____

¿Qué rutas están presentes en la tabla BGP de Router C?

_____
_____
_____
_____

¿Qué rutas BGP están presentes en la tabla de enrutamiento de Router C?

_____
_____
_____
_____

# CAPÍTULO DOS

## Índice laboratorio N° 2



## Índice de Figuras



## Índice de Tablas

# 2. LABORATORIO N° 2 - SISTEMA AUTÓNOMO DE TRÁNSITO

## 2.1. INTRODUCCIÓN

Un Sistema Autónomo de Tránsito es un Sistema Autónomo que contiene más de una conexión al mundo exterior y ofrece servicios de transporte para el tráfico originado desde otros ASs, encargándose del intercambio de información de enrutamiento BGP con otros sistemas autónomos, reenviando la información recibida desde un AS a otro AS.[3]

Todos los Sistemas Autónomos de Transito están obligados a transportar tráfico desde o destinados a ubicaciones fuera de ese sistema autónomo. Para lograr este objetivo es necesario que exista un grado de interacción entre BGP y el IGP que se ejecuta al interior del sistema autónomo.[4]

Este Laboratorio está orientado a comprender a fondo el funcionamiento de un sistema autónomo de tránsito además de entender el intercambio de información de enrutamiento BGP al interior del sistema autónomo y entre ASs.

3 Cisco Systems Learning.Configuring BGP on Cisco Routers. Volume 1. Versión 3.2. Estados Unidos. 2005. p. 34

4 Ibíd., p. 147.

## 2.2. OBJETIVOS

- Diseñar y documentar un esquema de direccionamiento según los requisitos.
- Configurar el enrutamiento RIPv2 en ambos Sistemas Autónomos.
- Configurar el enrutamiento EIGRP al interior del AS de tránsito.
- Configurar una malla completa de sesiones IBGP en cada AS.
- Configurar EBGP entre el AS de tránsito y ambos ASs.
- Verificar el correcto funcionamiento de los procesos BGP.
- Verificar la completa conectividad entre todos los dispositivos de la topología.

## 2.3. DIAGRAMA DE TOPOLOGÍA

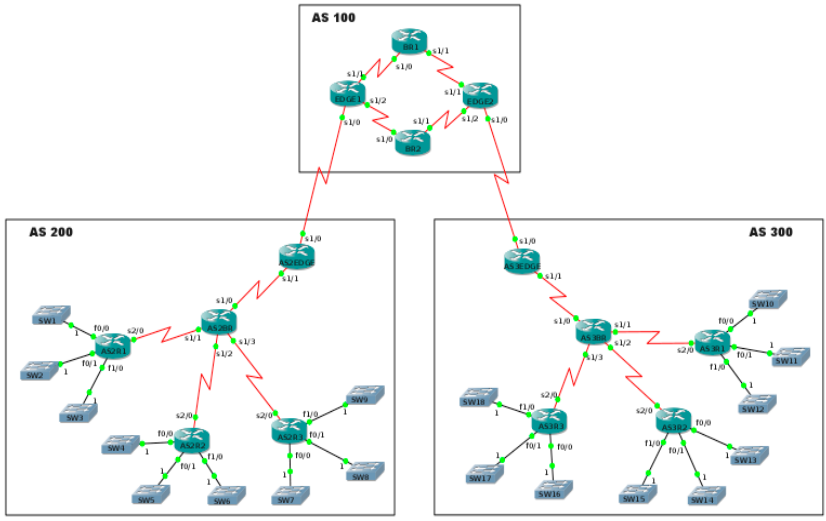


***Figura 2.1.*** Topología Sistema Autónomo de Tránsito

## 2.4. TABLAS DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Mascara de Subred |
|---|---|---|---|
| **EDGE1** | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback 0 | | |
| **EDGE2** | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback 0 | | |
| **BR1** | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback 0 | | |
| **BR2** | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback 0 | | |

Tabla 2.1. AS de Tránsito

| Dispositivo | Interfaz | Dirección IP | Mascara de Subred |
|---|---|---|---|
| **AS2EDGE** | Serial 1/0 | | |
| | Serial 1/1 | | |
| **AS2BR** | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| **AS2R1** | Serial 2/0 | | |
| | FastEthernet0/0 | | |
| | FastEthernet0/1 | | |
| | FastEthernet1/0 | | |
| **AS2R2** | Serial 2/0 | | |
| | FastEthernet0/0 | | |
| | FastEthernet0/1 | | |
| | FastEthernet1/0 | | |
| **AS2R3** | Serial 2/0 | | |
| | FastEthernet0/0 | | |
| | FastEthernet0/1 | | |
| | FastEthernet1/0 | | |

Tabla 2.2 AS de Tránsito [AS 200]

| Dispositivo | Interfaz | Dirección IP | Mascara de Subred |
|---|---|---|---|
| **AS3EDGE** | Serial 1/0 | | |
| | Serial 1/1 | | |
| **AS3BR** | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| **AS3R1** | Serial 2/0 | | |
| | FastEthernet0/0 | | |
| | FastEthernet0/1 | | |
| | FastEthernet1/0 | | |
| **AS3R2** | Serial 2/0 | | |
| | FastEthernet0/0 | | |
| | FastEthernet0/1 | | |
| | FastEthernet1/0 | | |
| **AS3R3** | Serial 2/0 | | |
| | FastEthernet0/0 | | |
| | FastEthernet0/1 | | |
| | FastEthernet1/0 | | |

Tabla 2.3. AS de Tránsito [AS 300]

## 2.5. DESCRIPCIÓN DE LA ACTIVIDAD

### TAREA 1: Diseñar y documentar un esquema de direccionamiento

**Paso 1:** Diseñe un esquema de direccionamiento.

Utilice la topología y los siguientes requisitos para diseñar un esquema de direccionamiento:

El espacio de dirección para la Región 200 es 172.16.128.0/17. Deberá asignar a cada router de sucursal (AS2R1, AS2R2, AS2R3) un espacio de dirección según estos requisitos comenzando por el requisito mayor.

Asigne un espacio de direccionamiento a cada router.
AS2R1 necesita espacio para 16 000 hosts _____
AS2R2 necesita espacio para 8000 hosts _____
AS2R3 necesita espacio para 4000 hosts _____

Divida el espacio de dirección para cada router de sucursal en tres subredes iguales.

| Dispositivo | Interfaz | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|---|
| AS2R1 | f 0/0 | 0 | | |
| | f 0/1 | 1 | | |
| | f 1/0 | 2 | | |

| Dispositivo | Interfaz | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|---|
| AS2R2 | f 0/0 | 0 | | |
| | f 0/1 | 1 | | |
| | f 1/0 | 2 | | |

| Dispositivo | Interfaz | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|---|
| AS2R3 | f 0/0 | 0 | | |
| | f 0/1 | 1 | | |
| | f 1/0 | 2 | | |

- Para las conexiones WAN en la Red del AS 200 utilice la dirección 172.16.240.0/28. La conexión AS2BR a AS2EDGE utiliza la primera subred, la conexión AS2BR a AS2R1 utiliza la segunda, la conexión AS2BR a AS2R2, la tercera y la conexión AS2BR a AS2R3 la cuarta subred.

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| AS2R1 <> AS2BR | 0 | | |
| AS2R2 <> AS2BR | 1 | | |
| AS2R3 <> AS2BR | 2 | | |
| AS2EDGE <> AS2BR | 3 | | |

- El espacio de dirección para la Red del AS 300 es 10.3.0.0/16. Deberá asignar a cada router de sucursal (AS3R1, AS3R2, AS3R3) un espacio de dirección según estos requisitos. Comenzando por el requisito mayor.

Asigne un espacio de direccionamiento a cada router.

- AS3R1 necesita espacio para 32000 hosts _____
- AS3R2 necesita espacio para 16000 hosts _____
- AS3R3 necesita espacio para 8000 hosts _____

Divida el espacio de dirección para cada router de sucursal en tres subredes iguales.

| Dispositivo | Interfaz | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|---|
| AS3R1 | f 0/0 | 0 | | |
| | f 0/1 | 1 | | |
| | f 1/0 | 2 | | |

| Dispositivo | Interfaz | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|---|
| AS3R2 | f 0/0 | 0 | | |
| | f 0/1 | 1 | | |
| | f 1/0 | 2 | | |

| Dispositivo | Interfaz | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|---|
| AS3R3 | f 0/0 | 0 | | |
| | f 0/1 | 1 | | |
| | f 1/0 | 2 | | |

- Para las WAN en la Red del AS 300, realice una conexión con una subred en la dirección 10.3.224.0/28. La conexión AS3BR a AS3EDGE utiliza la primera subred, la conexión AS3BR a AS3R1 utiliza la segunda, la conexión AS3BR a AS3R2, la tercera y la conexión AS3BR a AS3R3 la cuarta subred.

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| AS3R1 <> AS3BR | 0 | | |
| AS3R2 <> AS3BR | 1 | | |
| AS3R3 <> AS3BR | 2 | | |
| AS3EDGE <> AS3BR | 3 | | |

- Utilice el espacio de dirección 192.168.1.0.0/27 tanto para los enlaces al interior del sistema autónomo de transporte como para las subredes que lo conectan con las redes de los ASs 200 y 300. La conexión EDGE1 a AS2EDGE y la conexión EDGE2 a AS3EDGE utilizan la primera y segunda subred respectivamente. La conexión EDGE1 a BR1 utiliza la tercera subred, la conexión EDGE1 a BR2 utiliza la cuarta, la conexión EDGE2 a BR1 la quinta y por último la conexión EDGE2 a BR2 utiliza la cuarta subred.

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| EDGE1 <> AS2EDGE | 0 | | |
| EDGE2 <> AS3EDGE | 1 | | |
| EDGE1 <> BR1 | 2 | | |
| EDGE1 <> BR2 | 3 | | |
| EDGE2 <> BR1 | 4 | | |
| EDGE2 <> BR2 | 5 | | |

**Paso 2:** Documente el esquema de direccionamiento.

Documente las direcciones IP y máscaras de subred utilizando las tablas proporcionadas. Para las sucursales asigne la dirección IP más utilizable a la interfaz del router.

En los enlaces WAN asigne la primera dirección IP a AS2BR y AS3BR para los enlaces con los routers de borde (AS2EDGE y AS3EDGE) y los enlaces a cada router de sucursal para cada AS respectivo.

## TAREA 2: Preparación básica de la red

**Paso 1:** Conecte una red que sea similar a la del diagrama de topología.

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en el gráfico.

**Paso 2:** Configuración básica de los enrutadores.

Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautas generales (utilice como contraseña la palabra *"nyquist"*):

1. Configure el nombre de host del router.
2. Configure una contraseña de modo EXEC privilegiado.
3. Configure un mensaje del día.
4. Configure una contraseña para las conexiones de la consola.
5. Configure una contraseña para las conexiones de VTY.

## TAREA 3: Configurar el enrutamiento RIPv2 en la redes de ambos ASs (AS 200 y AS 300)

Configure el enrutamiento RIPv2 en todos los dispositivos de ambos ASs. En la configuración asegúrese de:

- Desactivar la sumarización automática.
- Detener las actualizaciones de enrutamiento en las interfaces adecuadas.

**Nota:** Los router usan un mecanismo de **búsqueda de enrutamiento recursiva** para determinar cómo enviar paquetes hacia destinos externos. Para conseguir que este mecanismo funcione los routers del AS deben resolver todas las direcciones IP *next-hop* a las que se hace referencia en sus tablas de enrutamiento IP, incluso las redes que conectan los ASs entre sí.[5]

Básicamente existen dos formas de hacer que el IGP que se ejecuta al interior del AS, transporte la información necesaria para resolver las direcciones de siguiente salto:

- Asegurarse que todos los routers de borde que contienen sesiones EBGP redistribuyan las subredes conectadas que hacen posible la comunicación con otros ASs en el IGP usando el protocolo redistributeconnected en el modo de configuración de router.

- Un método alternativo es incluir la subred en la cual se está ejecutando la sesión EBGP en la configuración IGP mediante el comando network. Para evitar que el router de borde intercambie información de enrutamiento IGP con el otro AS, debe configurar la interface como una interface pasiva.

Para ilustrar estos dos métodos configure el router de borde del AS 200 implementando el primer método planteado y configure el router de borde del AS 300 empleando el segundo.

## TAREA 4: Configurar el enrutamiento EIGRP en el AS de Tránsito

Configure todos los dispositivos con el protocolo de enrutamiento EIGRP en el Sistema Autónomo de Tránsito. En la configuración, asegúrese de:

- Desactivar la sumarización automática.
- Detener las actualizaciones de enrutamiento en las interfaces que no estén conectadas a los vecinos de EIGRP.

5 Cisco Systems Learning.Configuring BGP on Cisco Routers. Volume 1. Version 3.2. Estados Unidos. 2005. p. 167.

## TAREA 5: Configuración de sesiones BGP

"Aunque es un protocolo de Gateway exterior, también puede utilizarse dentro de un AS como un conducto para intercambiar actualizaciones BGP. Las conexiones BGP entre routers dentro de un sistema autónomo son denominadas BGP interno (IBGP), mientras que las conexiones BGP entre routers en sistemas autónomos separados son denominadas BGP externas (EBGP). Los routers que están utilizando IBGP se denominan routers de tránsito cuando transportan el tráfico de tránsito que va a través del AS."[6]

## TAREA 5.1: Configurar mallas completas de sesiones IBGP en ambos ASs y en el AS de tránsito

Para el establecimiento de sesiones IBGP utilice el siguiente comando de configuración de router asegurándose que la sesión se establezca con un vecino que pertenezca al mismo AS.

**neighbor** *ip-address* **remote-as***as-number*

Las reglas de horizonte dividido establecen que la información de enrutamiento recibida a través de una sesión IBGP nunca debe enviarse a otro vecino IBGP, sólo hacia vecinos EBGP; por lo tanto cada router dentro del sistema autónomo debe ser directamente actualizado por los routers frontera. Cada router al interior del sistema autónomo debe tener sesiones IBGP con cada router frontera, formando de este modo una malla completa de sesiones IBGP.[7]

En conclusión, todos los routers dentro del AS deben tener sesiones IBGP con los gateways, debido a que cada router sobre la ruta de tránsito dentro del AS debe tener información de enrutamiento sobre todas redes externas recibidas por los routers de borde.

**Paso 1:** Configurar una malla completa de sesiones IBGP en el AS 200

- Desde el router de borde AS2EDGE establezca sesiones IBGP a los demás routers del AS.
- Desde los routers de sucursal AS2R1, AS2R2 y AS2R3 establezca sesiones IBGP con el router frontera.

6 HALABI, Sam; MCPHERSON, Danny. Arquitectura de enrutamiento en Internet. SegundaEdición. Pearson Education.España. 2001. p. 98.

7 Cisco Systems Learning.Configuring BGP on Cisco Routers.Volume 1. Version 3.2. Estados Unidos. 2005. p. 160.

**Paso 2:** Establezca una malla completa de sesiones IBGP en el AS 300.

- Desde el router de borde AS3EDGE establezca sesiones IBGP a los demás routers del AS.
- Desde los routers de sucursal AS3R1, AS3R2 y AS3R3 establezca sesiones IBGP con el router frontera.

**Paso 3:** Configurar una malla completa de sesiones IBGP en el AS de tránsito.

**Paso 3.1:** Configurar sesiones IBGP desde los routers EDGE a todos los demás routers del AS de tránsito:
Establezca la relación de vecinos desde los routers de borde EDGE1 y EDGE2 hacia los demás routers del AS de tránsito.

La mejor elección al configurar sesiones IBGP en un AS de tránsito es establecer cada sesión entre interfaces *Loopback* en cada router BGP. Las sesiones IBGP que se establecen entre interfaces *Loopback* tienen una mayor estabilidad ya que no están sujetas a fallos de las interfaces físicas del router, por lo tanto, el fallo de estos enlaces no afectan la conectividad de la red.[8]

Utilice el siguiente comando de configuración de router para cada vecino en el AS de tránsito:

**neighbor**[*ip-address* | *peer-group-name*] **update-source** *interface*

**Nota:** Para mejorar el mecanismo de búsqueda recursiva puede utilizar el comando:

**neighbor**[*ip-address* | *peer-group-name*]**next-hop-self**

Este comando permite configurar un router IBGP para emular el comportamiento de una sesión EBGP sobre las sesiones IBPG de los routers de borde, permitiendo que las actualizaciones BGP recibidas a través de las sesiones EBGP sean reenviadas sobre las sesiones IBGP configurando el atributo **Next-Hop** con la dirección IP de origen de esta sesión IBGP, es decir, la dirección IP usada en el lado local de la sesión IBGP. El atributo **Next-Hop** original, establecido en el otro extremo de la sesión EBGP se perderá.[9]

Para ilustrar este método configure los routers de borde del Sistema Autónomo de Tránsito con este comando. (No incluya las subredes que conecta el AS de tránsito con ambos AS en el proceso de enrutamiento EIGRP).

8 Cisco Systems Learning.Configuring BGP on Cisco Routers.Volume 1. Version 3.2. Estados Unidos. 2005. p. 164.

9 Ibíd., p. 169.

**Paso 3.2:** Configurar sesiones IBGP desde los routers BR1 y BR2 hacia los routers frontera del AS de tránsito.

## TAREA 6: Establecer las sesiones EBGP entre el AS de tránsito y los ASs 200 y 300

Para el establecimiento de sesiones EBGP utilice el siguiente comando de configuración de router asegurándose que el AS vecino es diferente al AS local.

**neighbor** *ip-address* **remote-as** *as-number*

**Paso 1:** Configurar las sesión EBGP entre al AS de tránsito y el AS 200.
Establezca la relación de vecinos externa desde el router de borde EDGE1 hacia el router de borde del sistema autónomo 200.

**Paso 2:** Configurar las sesión EBGP entre al AS de tránsito y el AS 300.

Establezca la relación de vecinos externa desde el router de borde EDGE2 hacia el router de borde del sistema autónomo 300.

## TAREA 7: Anunciar las redes desde ambos AS al AS de tránsito

Utilice el siguiente comando de configuración de router:

**network** *ip-prefix-address*[**mask***subnet-mask*]

**Paso 1:** Anuncie el espacio de dirección para la Región 200 desde su router de borde.

Anuncie la red 172.16.128.0/17 desde el router de borde del AS 200 y cree una ruta estática coincidente con esta red que apunte a la interfaz *null0*.

**Paso 1:** Anuncie el espacio de dirección para la Región 300 desde su router de borde.

Anuncie la red 10.3.0.0/16 desde el router de borde del AS 300 y cree una ruta estática coincidente con esta red que apunte a la interfaz *null0*.

¿Averigüe por qué es importante establecer rutas estáticas apuntando a la interface *null0*?

_____

_____

_____

_____

## TAREA 8: Verificar la completa conectividad entre todos los dispositivos de la topología

**Paso 1:** Pruebe la conectividad.

- Ahora debe tener conectividad entre ambos ASs. Utilice el ping para probar la conectividad. ¿Cada router tiene respuesta al realizar un ping a todas las otras interfaces de cada router local y remoto del As? SI __ NO ___
- Resuelva los problemas que se presenten hasta que los pings tengan éxito.

**Paso 2:** Examine la configuración.

Utilice los comandos de verificación para asegurarse de haber completado sus configuraciones.

**REFLEXIÓN FINAL**

Como puede ver el AS de tránsito no fue configurado para anunciar sus redes hacia los AS 200 y 300. ¿Cree que el no hacerlo puede ocasionar fallas de conectividad entre ambos ASs? Justifique su respuesta.

# CAPÍTULO TRES

# Índice laboratorio N° 3



# Índice de Figuras



# Índice de Tablas

# 3. LABORATORIO N° 3 –ENRUTAMIENTO BASADO EN POLÍTICAS DE CONTROL

## 3.1. INTRODUCCIÓN

En búsqueda de una conexión altamente redundante a Internet, las compañías pueden considerar contratar servicios con dos ISP diferentes o tener dos conexiones separadas a un mismo ISP, consiguiendo a través de la primera opción una redundancia completa.

Este enfoque requiere que los clientes sean responsables de aplicar sus propias políticas y anunciar sus redes IP hacia Internet, y sin la implementación de ningún tipo de filtrado, toda la información de enrutamiento de BGP creada desde el AS del cliente puede potencialmente ser propagada sobre todo Internet. De este modo, el cliente puede inyectar información errónea dentro de las tablas de enrutamiento de Internet.

El enrutamiento basado en políticas es un medio para controlar rutas que dependen del origen, o del origen y del destino, o del tráfico en lugar de sólo el destino. El enrutamiento basado en políticas puede ser utilizado para controlar el tráfico dentro de un AS o entre varios AS. Se utiliza cuando es necesario forzar el comportamiento de enrutamiento diferente de lo que dictan los protocolos de enrutamiento dinámico.

## 3.2. OBJETIVOS

- Influenciar el proceso de selección de rutas de BGP utilizando listas de acceso basadas en el atributo AS-Path.
- Influenciar el proceso de selección de rutas de BGP utilizando listas de prefijos.
- Utilizar la funcionalidad ORF para minimizar el impacto de las actualizaciones de enrutamiento sobre los recursos de los routers.
- Influenciar el proceso de selección de rutas de BGP utilizando Route-Maps.
- Implementar la reconfiguración del proceso BGP.

## 3.3. DIAGRAMA DE TOPOLOGÍA

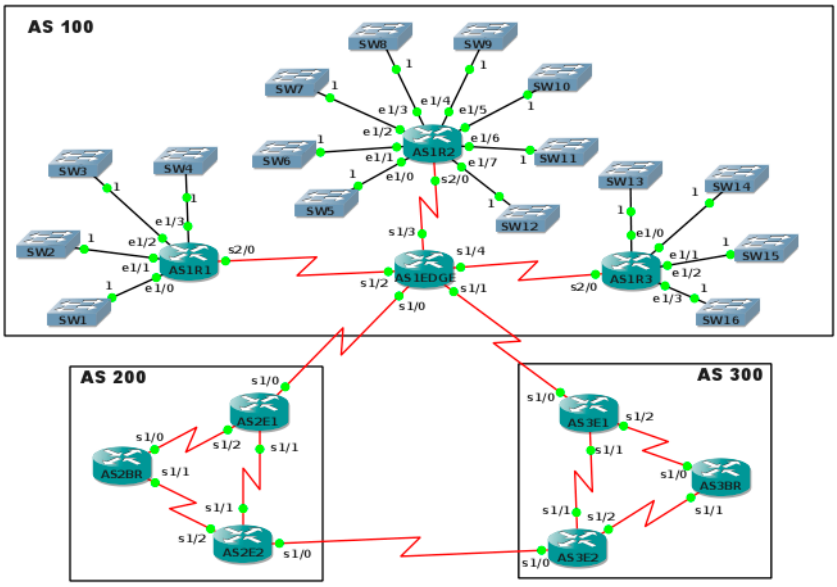


***Figura 3.1.*** Topología Enrutamiento Basado en Políticas

## 3.4. TABLAS DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| AS1EDEGE | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Loopback0 | | |
| AS1R1 | Ethernet 1/0 | | |
| | Ethernet 1/1 | | |
| | Ethernet 1/2 | | |
| | Ethernet 1/3 | | |
| | Serial 2/0 | | |
| | Loopback0 | | |
| AS1R2 | Ethernet 1/0 | | |
| | Ethernet 1/1 | | |
| | Ethernet 1/2 | | |
| | Ethernet 1/3 | | |
| | Ethernet 1/4 | | |
| | Ethernet 1/5 | | |
| | Ethernet 1/6 | | |
| | Ethernet 1/7 | | |
| | Serial 2/0 | | |
| | Loopback0 | | |
| AS1R3 | Ethernet 1/0 | | |
| | Ethernet 1/1 | | |
| | Ethernet 1/2 | | |
| | Ethernet 1/3 | | |
| | Serial 2/0 | | |
| | Loopback 0 | | |

Tabla 3.1 Enrutamiento Basado en Políticas [AS 100]

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| AS2E1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback0 | | |
| AS2E2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback0 | | |
| AS2BR | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |

Tabla 3.2. Enrutamiento Basado en Políticas [AS 200]

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| AS3E1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback0 | | |
| AS3E2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback0 | | |
| AS3BR | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |

Tabla 3.3. Enrutamiento Basado en Políticas [AS 300]

## 3.5. DESCRIPCIÓN DE LA ACTIVIDAD

### TAREA 1: División en subredes del espacio de direccionamiento

**Paso 1:** Examinar los requisitos de la red.

El direccionamiento para la red tiene los siguientes requisitos:

- Para el AS 100, se ha definido el espacio de direcciones privadas 172.16.0.0/20, para proporcionar direcciones a las LAN del router AS1R1, las cuales no deben ser publicadas fuera del AS. El router sucursal AS1R1 requerirá un espacio de direcciones para 4.000 hosts, el cual deberá ser dividido en cuatro subredes iguales.

| Dispositivo | Interfaz | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|---|
| AS1R1 | Ethernet 1/0 | 0 | | |
| | Ethernet 1/1 | 1 | | |
| | Ethernet 1/2 | 2 | | |
| | Ethernet 1/3 | 3 | | |

- Adicionalmente, se asignó el espacio de direcciones públicas 100.128.0.0/17, el cual puede ser publicado a los demás AS y debe dividirse en subredes para proporcionar direcciones a las LAN de los routers AS1R2 y AS1R3:
    - El router sucursal AS1R2 requerirá un espacio de direcciones para 16.000 hosts. Divida el espacio de direcciones para el router sucursal AS1R2 en ocho subredes iguales.

| Dispositivo | Interfaz | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|---|
| AS1R2 | Ethernet 1/0 | 0 | | |
| | Ethernet 1/1 | 1 | | |
| | Ethernet 1/2 | 2 | | |
| | Ethernet 1/3 | 3 | | |
| | Ethernet 1/4 | 4 | | |
| | Ethernet 1/5 | 5 | | |
| | Ethernet 1/6 | 6 | | |
| | Ethernet 1/8 | 7 | | |

- El router sucursal AS1R3 requerirá un espacio de direcciones para 8.000 hosts. Divida el espacio de direcciones para el router sucursal AS1R3 en cuatro subredes iguales.

| Dispositivo | Interfaz | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|---|
| AS1R3 | Ethernet 1/0 | 0 | | |
| | Ethernet 1/1 | 1 | | |
| | Ethernet 1/2 | 2 | | |
| | Ethernet 1/3 | 3 | | |

- Para las interfaces Loopbacky los enlaces Seriales al interior del AS se utiliza el espacio de direcciones privadas 192.168.0.192/28, el cual debe dividirse en subredes.
  - Los enlaces seriales internos entre los routers requerirán dos direcciones para cada enlace.
  - Las interfaces Loopback por cada router requerirán una sola dirección IP.

| **Conexión** | **No. de Subred** | **Dirección Subred** | **Máscara Subred** |
|---|---|---|---|
| AS1EDGE <> AS1R1 | 0 | | |
| AS1EDGE <> AS1R2 | 1 | | |
| AS1EDGE <> AS1R3 | 2 | | |

- Para el AS 200 se ha sido asignado el espacio de direcciones 192.168.0.0/28, el cual debe dividirse en subredes para proporcionar direcciones a las interfaces Loopback y los enlaces seriales internos.

  - Los enlaces seriales entre los routers requerirán dos direcciones para cada enlace.
  - Las interfaces Loopback por cada router requerirán una sola dirección IP.

| **Conexión** | **No. de Subred** | **Dirección Subred** | **Máscara Subred** |
|---|---|---|---|
| AS2E1 <> AS2E2 | 0 | | |
| AS2E1 <> AS2BR | 1 | | |
| AS2E2 <> AS2BR | 2 | | |

- Para el AS 300 ha sido asignado el espacio de direcciones 10.0.0.0/28, el cual debe dividirse en subredes para proporcionar direcciones a las interfaces Loopback y los enlaces seriales internos.

  - Los enlaces seriales entre los routers requerirán dos direcciones para cada enlace.
  - Las interfaces Loopback por cada router requerirán una sola dirección IP.

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| AS3E1 <> AS3E2 | 0 | | |
| AS3E1 <> AS3BR | 1 | | |
| AS3E2 <> AS3BR | 2 | | |

- Para las conexiones externas entre los AS se ha asignado la red 209.128.0.0/28.

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| AS1EDGE <> AS2E1 | 0 | | |
| AS1EDGE <> AS3E1 | 1 | | |
| AS2E2 <> AS3E2 | 2 | | |

**Paso 2:** Documente el esquema de direccionamiento.

Documente las direcciones IP y máscaras de subred utilizando las tablas proporcionadas. Para las sucursales asigne la dirección IP más utilizable a la interfaz del router.

## TAREA 2: Preparación básica de la red

**Paso 1:** Conecte una red que sea similar a la del diagrama de topología.

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en el gráfico.

**Paso 2:** Configuración básica de los enrutadores.

Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautas generales (utilice como contraseña la palabra *"nyquist"*):

1. Configure el nombre de host del router.
2. Configure una contraseña de modo EXEC privilegiado.
3. Configure un mensaje del día.
4. Configure una contraseña para las conexiones de la consola.
5. Configure una contraseña para las conexiones de VTY.

## TAREA3: Configurar y activar interfaces de los dispositivos

**Paso 1:** Configure las interfaces en los enrutadores con las direcciones IP de la tabla proporcionada debajo del Diagrama de topología.

## TAREA 4: Configurar el protocolo de enrutamiento interno

**Paso 1:** Configurar el enrutamiento RIPv2 en cada uno de los routers del AS 100.

Configure el enrutamiento RIPv2 en todos los dispositivos del AS 100. En la configuración asegúrese de:

- Desactivar la sumarización automática.
- Gracias a que se utilizó explícitamente un espacio de direccionamiento privado para los enlaces seriales internos y las interfaces Loopback, utilice el comando network junto con el espacio de direcciones de estas interfaces (192.168.0.192/28) para establecer las interfaces que participaran en el enrutamiento RIPv2.
- Redistribuir las redes de las interfaces directamente conectadas en las actualizaciones del enrutamiento RIP.

**Consulte y analice:** ¿Será necesario detener las actualizaciones del IGP por alguna de las interfaces que no participan en el enrutamiento?

_____

_____

_____

_____

**Paso 2:** Configurar el enrutamiento OSPF en cada uno de los routers del AS 200.

Configure todos los dispositivos con un enrutamiento OSPF en el AS 200. En la configuración, asegúrese de:

- Utilizar el Id de proceso 1 y el área 0 para las redes.
- Al igual que en el AS 100, se utilizó explícitamente un espacio de direccionamiento privado para los enlaces seriales internos y las interfaces Loopback, se anuncia el espacio de direcciones de estas interfaces (192.168.0.0/28) para establecer las interfaces que participaran en el enrutamiento OSPF.
- Redistribuir las redes de las interfaces directamente conectadas en las actualizaciones del enrutamiento OSPF.

**Paso 3:** Configurar el enrutamiento EIGRP en cada uno de los routers del AS 300.

Configure todos los dispositivos con un enrutamiento EIGRP en el AS 300. En la configuración, asegúrese de:

- Utilizar el Id de proceso 1.
- Desactivar la sumarización automática.
- Igual que en el AS 100 y el AS 200, se anuncia el espacio de direcciones de las interfaces seriales internas y Loopback (10.0.0.240/28) para establecer las interfaces que participaran en el enrutamiento EIGRP.
- Redistribuir las redes de las interfaces directamente conectadas en las actualizaciones del enrutamiento EIGRP.

## TAREA 5: Configurar el enrutamiento BGP en cada uno de los ASs

**Paso 1:** Configurar mallas completas de sesiones IBGP entre interfaces *Loopback* al interior de los ASs.

Establezca sesiones IBGP para el AS 100, el AS 200 y el AS 300, a partir de las interfaces *Loopback* de los router.

**Paso 2:** Establecer sesiones EBGP.

Las sesiones EBGP entre ASs sólo se deben establecer entre los routers de borde entre interfaces directamente conectadas.

**Paso 3:** Habilitar la publicación de redes al interior de los ASs.

Configure la red 192.168.1.0/24 sobre la interfaz *Loopback 1*del router AS2BR, redistribúyala sobre el IGP que corre al interior del AS, y publíquela desde el router AS2EDGE1.

Configure la red 10.1.0.0/16 sobre la interfaz *Loopback 1*del router AS3BR, redistribúyala sobre el IGP que corre al interior del AS, y publíquela desde el router AS3EDGE1.

**Nota:** Como pudo observar, las configuraciones realizadas hasta este punto no difieren de las realizadas en el laboratorio anterior. Sin embargo, el objetivo de este laboratorio no es el de configurar un AS de tránsito, sino un cliente (AS 100) *multihomed*, es decir, que ha contratado servicio de conectividad con un par de ISPs (AS 200 y AS 300).
**Consulte y analice:**

¿Qué tipo de consecuencias traerá para el cliente, el habilitar su propio AS para prestar servicios de transporte y permitir el intercambio de información entre ISPs?

¿Qué se podría implementar sobre el AS del cliente para evitar esta problemática?

**Paso 4:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

¿Es posible realizar un ping desde la interfaz *Loopback1* del router AS2BR a la interfaz *Loopback 1* del router AS3BR? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 1* del router AS3BR a la interfaz *Loopback 1* del router AS2BR? SI ___ NO ___

¿Qué rutas BGP están presentes en la tabla de BGP del router AS1EDGE?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS2EDGE1?

¿Qué rutas están presentes en la tabla de BGP del router AS3EDGE1?

## TAREA6: Implementación de listas de acceso basadas en el atributo AS-Path

La solución más óptima para no permitir que el AS del cliente se comporte como un AS de tránsito, es implementar filtros que descarten cualquier paquete destinado hacia otro AS diferente, que haya sido originado fuera del AS del cliente, es decir, que sólo permitan la salida de paquetes localmente originados.

Teniendo en cuenta esta implementación se puede evitar al interior del AS del cliente cualquier cantidad de problemas, tanto de sobrecarga de recursos de procesamiento y memoria en los routers, como de saturación indeseada de ancho de banda sobre los enlaces que se comparten con los ISPs, debido a la extensa lista de redes de Internet presentes en las tablas de BGP de estos últimos, y a la cantidad de actualizaciones necesarias para mantener una tabla de BGP de estas dimensiones.

**Nota:** Tenga en cuenta que las problemáticas anteriormente mencionadas sólo pueden presentarse siempre y cuando el AS del cliente sea *multihomed*, es decir, que comparta enlaces directamente conectados con diferentes ISPs, sobre los cuales se podría permitir el intercambio de paquetes de un ISP a otro; en un ambiente en el que el cliente sea *single-homed* no se presenta esta situación, y por tanto, no es necesario implementar la solución mencionada en esta sección.

Como se pudo observar en las tablas de enrutamiento de los ASs que se consideran como ISPs (AS 200 y AS 300), para la topología de este laboratorio, las rutas utilizadas para alcanzar las redes anunciadas por estos ASs, no son a través del AS del cliente, esto es debido a que ambos ASs comparten enlaces directamente conectados. Sin embargo, esto no significa que el AS del cliente (AS 100) no se esté comportando como un AS de tránsito. Esto se puede comprobar observando la tabla BGP de los routers en el AS 200 y en el AS 300.

Si en el enlace que conecta directamente al AS 200 con el AS 300, se llegara a presentar alguna falla, automáticamente BGP en ambos ASs, descartará esta ruta para alcanzar las subredes mencionadas anteriormente. Luego elegirá la ruta a través del AS del cliente como la mejor, e indexará dicha ruta en la tabla de enrutamiento, para posteriormente publicarla sobre todas las sesiones IBGP y EBGP, permitiendo el paso de paquetes desde el AS 200 hacia el AS 300, con el AS del cliente como intermediario.

Para que un router pueda identificar un conjunto de rutas específicas, basándose en el AS que fue originada o en los AS determinados que ha atravesado, es necesario referirse al atributo ***AS-Path***. Este atributo se presenta como una secuencia de números, cada uno de ellos indica un AS que la ruta ha atravesado. Cuando una ruta es originada, el atributo ***AS-Path*** es creado y se deja vacío hasta que la ruta cruce la frontera del AS local, y sea publicado por un router de borde a otro AS. Cada vez que la ruta cruza la frontera de un AS, el router de borde antepone su número AS en el atributo ***AS-Path*** de esta ruta.
Las listas de acceso basadas en el atributo ***AS-Path***, se basan en el contenido de este para filtrar rutas, generando coincidencias a través de **expresiones regulares**.

**Paso 1:** Introducción a expresiones regulares.

Para hacer uso correcto de las listas de acceso basadas en el atributo ***AS-Path*** y obtener el resultado deseado de ellas, es necesario tener pleno conocimiento de la forma adecuada de implementar **expresiones regulares**. Por lo tanto, se realizarán diferentes ejercicios haciendo

uso del comando **show ipbgp** en un escenario que brindará un acercamiento a las tablas BGP reales que se utilizan en Internet.

Ingrese una dirección web que tenga un match con la cadena "BGP 4 looking Glass".

Diríjase al final de la página, en donde encontrará rutas de acceso para establecer sesiones *telnet* a routers reales en diferentes regiones del mundo. Seleccione un router, y establezca una sesión*telnet* con este.

Para concientizarse de la magnitud y extensión de Internet, utilice el comando **show ipbgp** y verifique el tamaño de la tabla de BGP del router con el que ha establecido una sesión*telnet*.

Para los siguientes ejercicios tenga en cuenta el siguiente comando, el cual permite imprimir en pantalla un subconjunto de redes de la tabla de BGP con base en una expresión regular:

**Showipbgpregexp**<*regular-expression*>

Realice los siguientes ejercicios sobre la tabla BGP del router al cual ha establecido una sesión BGP:

- Cree una expresión regular que contenga sólo un número de 4 cifras. Escriba la expresión regular:[0-9]{4}
- Cree una expresión regular que muestre las rutas que contengan un determinado número de AS en sus AS-Paths (Elija un número de AS de los vistos en la tabla BGP). Escriba la expresión regular: _200_
- Cree una expresión regular que muestre sólo las redes originadas por el AS anterior. Escriba la expresión regular: _200$
- Cree una expresión regular que muestre las rutas que son originadas por los vecinos AS directamente conectados. Escriba la expresión regular: ^100$|^200$
- Cree una expresión regular que muestre todas las rutas que son alcanzables por uno de los AS directamente conectados. Escriba la expresión regular: ^100_|^200_
- Cree una expresión regular que muestre todas las rutas que son originadas por los vecinos AS directamente conectados, y que posiblemente repita su número AS repetidamente en el AS-Path. Escriba la expresión regular: ^100_(100)*_$ | ^200_(200)*_$
- Cree una expresión regular que muestre las rutas que son originadas localmente. Escriba la expresión regular: ^$
- Cree una expresión regular que muestre todas las rutas, sin importar el contenido del atributo AS-Path. Escriba la expresión regular:.*

**Paso 2:** Configurar una lista de acceso basada en el *AS-Path.*

Configure una lista de acceso basada en el atributo ***AS-Path*** para filtrar rutas de acuerdo a las especificaciones anteriormente mencionadas para el AS del cliente, sobre el router AS1EDGE. Para llevar a cabo esta tarea tenga en cuenta el siguiente comando:

**ip as-path access-list** *access-list-number* {**permit | deny**} *regular-expression*

**Nota:** Tenga en cuenta que en las listas de acceso basadas en el atributo ***AS-Path***, las rutas que no generan ninguna coincidencia con las expresiones regulares que estas contienen son rechazadas implícitamente.

**Expresiones Regulares más comunes usadas en filtrado a través del atributo AS-Path**

Coincidencia con cualquier información de ruta
**.***
Coincidencia con rutas que inicien y finalicen con el AS n
**^n$**
Coincidencia con rutas originadas por el AS local
^$
Coincidencia con rutas que comienzan con el AS n, o actualizaciones provenientes desde el AS n
**^n_ | ^n_.***
Coincidencia con rutas que finalicen con el AS n, una ruta originada en el AS n
**_n$ | .*_n$**
Coincidencia con rutas que pasen a través del AS n
**_n_**
Coincidencia con rutas que pasen exactamente a través del AS n y luego AS m
_n m_

¿Cuál sería la expresión regular necesaria para satisfacer los requerimientos del cliente?

_____

_____

**Paso 3:** Aplicar la lista de acceso a vecinos BGP.

Aplique la lista de acceso a los vecinos determinados, en la dirección (**in**ó**out**) en que se deban filtrar las rutas de acuerdo a las especificaciones anteriormente mencionadas. Para realizar esta tarea tenga en cuenta el siguiente comando:

**Neighbor** *neighbor-ip-address* **filter-list** *access-list-number* {**in | out**}

**Nota:** Para que la lista de acceso basada en el atributo ***AS-Path*** recién configurada, sea

aplicada sobre las actualizaciones entrantes o salientes a los vecinos, es necesario reiniciar el intercambio de rutas entre ellos. Por lo tanto, utilice el siguiente comando del modo EXEC privilegiado, para reiniciar el intercambio de actualizaciones BGP entre vecinos.
Clear ip bgp

**Consulte y analice:**

¿Cuáles son las posibles alternativas para el comando **clear ipbgp**?

¿Cuáles son los requerimientos necesarios para utilizar estas alternativas?

¿Cuáles son las ventajas y desventajas de utilizar cada una de estas alternativas?

**Paso 4:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

¿Es posible realizar un ping desde la interfaz *Loopback 1* del router AS2BR a la interfaz *Loopback 1* del router AS3BR? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 1*del router AS3BR a la interfaz *Loopback 1* del router AS2BR? SI __ NO ___

¿Qué rutas BGP están presentes en la tabla de BGP del router AS1EDGE?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS1EDGE1?

¿Qué rutas están presentes en la tabla de BGP del router AS2EDGE1?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS2EDGE1?

¿Qué rutas están presentes en la tabla de BGP del router AS3DGE1?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS3EDGE1?

## TAREA 7: Implementación de listas de prefijos

Los clientes con redes *multihomed* son responsables de anunciar sus propias redes utilizando BGP. Normalmente, los clientes no son tan experimentados con BGP como lo son los ISPs, y por tanto es común que ocurran errores. Un ISP con un cliente *multihomed* tiene que tener precaución de no aceptar, utilizar o reenviar información de enrutamiento errónea recibida desde el cliente.

Al cliente se le asigna un espacio de direcciones IP que debe anunciar. Si el cliente anuncia cualquier red adicional, quiere decir que pudo haber cometido un error en la configuración de BGP. Por ejemplo, pudo haber olvidado no actuar como AS de tránsito y debe haber empezado a propagar rutas que han sido recibidas desde el otro proveedor de servicio o el cliente pudo haber empezado accidentalmente a enviar su espacio de direcciones privado, el cual es utilizado por el cliente para las direcciones de los enlaces, interfaces *Loopback*, u otros dispositivos que nunca deben tener acceso a Internet.

Para evitar problemas, el ISP puede aplicar un filtro de prefijo IP sobre la información entrante desde el cliente. El ISP sólo aceptará los números de red permitidos por la lista de prefijos.

**Paso 1:** Redistribuir enrutamiento del IGP a través de BGP.

Redistribuir en el AS1EDGE, el enrutamiento RIPv2 que se ejecuta al interior del AS 100 sobre BGP, para que este publique las rutas internas a los AS vecinos 200 y 300.
**Consulte y analice:**

¿Qué consecuencias trae para Internet el que un AS publique rutas de un espacio de direccionamiento privado utilizado internamente?

_____
_____
_____
_____

¿Qué entidad se encarga de regular que rutas pueden ser publicadas en Internet?

_____
_____
_____
_____

**Paso 2:** Verificar tablas BGP de los vecinos.

Verifique en las tablas de enrutamiento y de BGP, que el router AS1EDGE haya distribuido correctamente a los vecinos del AS 200 y el AS 300, todas las rutas aprendidas a través del enrutamiento RIPv2.

**Paso 3:** Configurar lista de prefijos para filtrar enrutamiento erróneo.

Como se pudo haber comprobado, el AS del cliente ha configurado inapropiadamente BGP, y está anunciando su propio direccionamiento privado. El ISP tiene la obligación de no permitir que esta información de enrutamiento errónea se propague sobre todo Internet. Por tanto el ISP debe filtrar toda la información entrante desde el cliente y aceptar únicamente aquella que se encuentra en el rango del espacio de direccionamiento asignado para el AS del cliente (100.128.0.0/17), el ISP debe descartar cualquier información fuera de los límites estrictos. De este modo, el ISP previene la propagación de información errónea al resto de la Internet.

Configure una lista de prefijos en ambos ISPs (AS 200 y AS 300) sobre los routers de borde respectivos, la cual filtre toda información de enrutamiento fuera de los límites estrictos del espacio de direccionamiento asignado al AS del cliente que puede ser publicado. Para llevar a cabo esta actividad haga uso del comando:

**ip prefix-list** *prefix-list-name* [**seq** *seq-value*] {**permit | deny**} *network-ip-address/len* [**ge** *ge-value*] [**le** *le-value*]

**Nota:** Tenga en cuenta que en las listas de prefijos, las rutas que no generan ninguna coincidencia con los prefijos que estas contienen, son rechazadas implícitamente.

**Paso 4:** Aplicar lista de prefijos a vecinos BGP.

Aplique la lista de prefijos a los vecinos determinados, en la dirección (**in** ó **out**) en que se deban filtrar las rutas de acuerdo a las especificaciones anteriormente mencionadas. Para realizar esta tarea tenga en cuenta el siguiente comando de configuración de router:

**Neighbor** *neighbor-ip-address* **prefix-list** *prefix-list-name* {**in | out**}

**Nota:** Para que la lista de prefijos recién configurada, sea aplicada sobre las actualizaciones entrantes o salientes a los vecinos, es necesario reiniciar el intercambio de rutas entre ellos. Por lo tanto, utilice el comando **clear ip bgp** (en cualquiera de sus posibles implementaciones) para reiniciar el intercambio de actualizaciones BGP entre vecinos.

**Paso 5:** Agregación de ruta para resumir direccionamiento del AS del cliente.

Algunos grandes ISP filtran rutas con prefijos largos. Los ISP no quieren llenar sus tablas de enrutamiento con un gran número de rutas explícitas que deberán haber sido incluidas en un resumen de ruta antes de que fueran enviadas.

Utilice la agregación de ruta sobre el AS del cliente para resumir rutas del espacio de direccionamiento designado a este de la siguiente forma:

- Utilice la agregación de ruta para obtener resúmenes de ruta con un prefijo de red: /20. ¿Cuáles serían las direcciones de red de los resúmenes de ruta resultantes?

  _____
  _____
  _____
  _____

- Utilice la agregación de ruta para obtener resúmenes de ruta con un prefijo de red: /19. ¿Cuáles serían las direcciones de red de los resúmenes de ruta resultantes?

  _____
  _____
  _____
  _____

- Utilice la agregación de ruta para obtener resúmenes de ruta con un prefijo de red: /18. ¿Cuáles serían las direcciones de red de los resúmenes de ruta resultantes?

  _____
  _____
  _____
  _____

- Utilice la agregación de ruta para obtener resúmenes de ruta con un prefijo de red: /17. ¿Cuáles serían las direcciones de red de los resúmenes de ruta resultantes?

  _____
  _____
  _____
  _____

**Paso 6:** Configurar lista de prefijos para filtrar rutas según especificaciones de los ISP.

- Para el AS 200:

- El ISP ha especificado que se deben filtrar rutas explícitas con prefijos mayores o iguales: /21. ¿Cuál sería la condición para esta lista de prefijo?

_____

- Además no desea tener resúmenes de ruta con un prefijo menor o iguales a: /17. ¿Cuál sería la condición para esta lista de prefijo?

_____

- Para el AS 300:

  - Se ha acordado con el ISP que el enlace que comparte con el AS del cliente será para conectividad de respaldo, por lo tanto, los resúmenes de ruta anunciados por este AS deben permitir que las rutas anunciadas por el AS 200 sean consideradas por otros AS como más específicas, y elijan el renvío de rutas hacia el AS del cliente a través del AS 200, considerado como el enlace primario. ¿Cuál sería la condición para esta lista de prefijo?

**Consulte y analice:**

¿Será esta la mejor o la única forma de configurar un enlace primario y un enlace secundario?

_____
_____
_____

¿Estarán los ISPs dispuestos a escuchar las peticiones de configuración individuales de cada uno de sus clientes? Justifique su respuesta.

_____
_____
_____

**Paso 7:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.
¿Es posible realizar un ping desde la interfaz *Loopback 1* del router AS2BR a cada una de las interfaces directamente conectadas a las LAN del router AS1R1? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 1* del router AS2BR a cada una de las interfaces directamente conectadas a las LAN del router AS1R2? SI __ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 1* del router AS2BR a cada una de las interfaces directamente conectadas a las LAN del router AS1R3? SI ___ NO ___

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS2EDGE1?

¿Qué rutas están presentes en la tabla de BGP del router AS2EDGE1?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS3EDGE1?

¿Qué rutas están presentes en la tabla de BGP del router AS2EDGE1?

En el router AS2EDGE1, deshabilite la interfaz directamente conectada al AS 100 con el comando ***shutdown***. Vuelva a realizar el proceso de verificación de las configuraciones y la conectividad. Una vez verificado el estado de la red, reactive la interfaz del router AS2EDGE1.

## TAREA 8: Apartado extra para implementación de la función ORF, y la optimización en el filtrado de información de enrutamiento de entrada

**ORF** (Outbound Route Filtering) es una característica de BGP basada en la publicación de capacidades ORF a routers pares. Cuando esta función está habilitada, un router configurado con BGP puede instalar un filtro ***prefix-list*** de entrada, en el par remoto como un filtro de salida, lo cual reduce las actualizaciones de enrutamiento. Este mecanismo reduce el consumo de ancho de banda y del uso de CPU cuando un router solicita una actualización de ruta. A continuación se presenta una ilustración para explicar la razón de usar ORF.

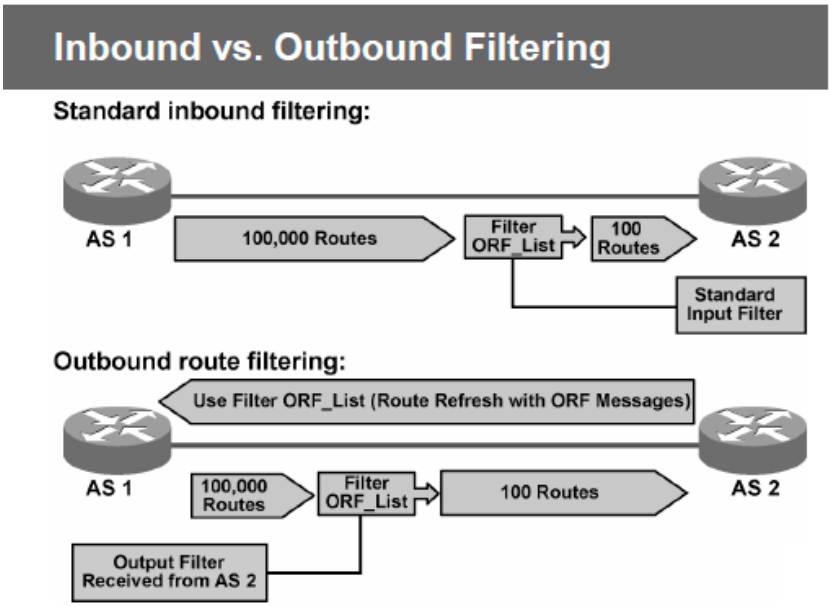


***Figura 3.2.*** Funcionamiento ORF

Apartado para implementación adicional de ORF. Se debe lograr obtener el mismo comportamiento que en el escenario anterior.

Cómo configurar el mecanismo ORF

Configure la función ORF sobre los routers de borde del AS 100, el AS 200 y el AS 300, en los cuales considere que es útil implementar este mecanismo. Para esto tenga en cuenta el siguiente comando:

**Neighbor** *neighbor-ip-address* **capability orf prefix-list** [**receive | send | both**]

El parámetro **send** es usado en el router que va a realizar la tarea de enviar la lista de prefijo a su vecino BGP. Mientras que el parámetro **receive** es para el vecino BGP que va a recibir el filtro y lo va a aplicar. A continuación se presenta un ejemplo de configuración de un par de routers BGP para un escenario con ORF.

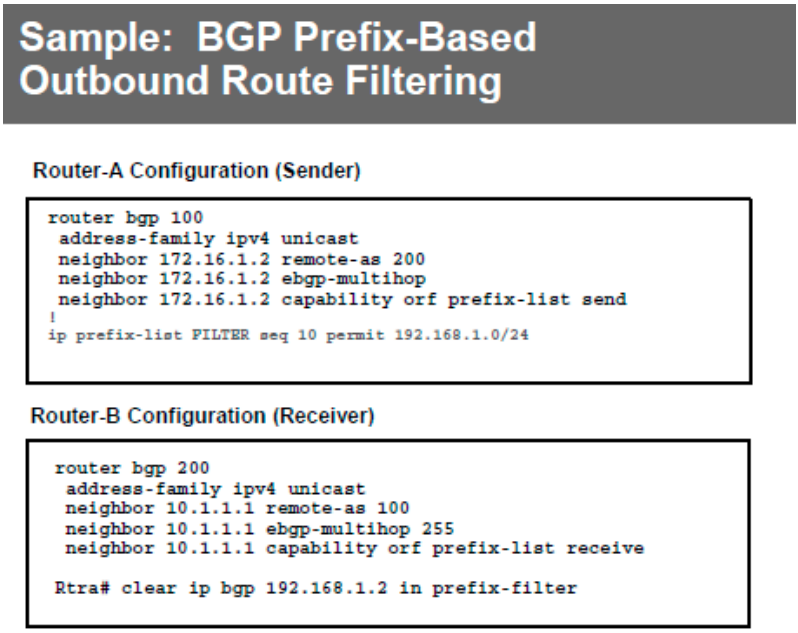


***Figura 3.3.*** Ejemplo de configuración ORF

El último comando en el router B reinicia la sesión con el vecino 192.168.1.2 para solicitar un inbound reconfiguration, es decir para generar un route refresh y pasar nuevamente las rutas por el filtro ORF instalado.

Para que el mecanismo ORF sea aplicado, es necesario reiniciar el intercambio de rutas entre los vecinos. Por lo tanto, utilice el siguiente comando para reiniciar el intercambio de actualizaciones BGP entre vecinos:

**Clearipbgp** {* | *neighbor-ip-address*} **in**

**Paso 2:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

Las tablas de enrutamiento y de BGP de los routers de borde no deben diferir de las analizadas en la actividad anterior.

## TAREA 9: Implementación de *Route-Maps* como filtros BGP

Los ***Route-Maps*** son utilizados por BGP para controlar y modificar información de enrutamiento y definir las condiciones por las cuales las rutas son redistribuidas entre dominios de enrutamiento, mediante clausulas **set** y **match**.

**Paso 1:** Configurar *Route-Map* para filtrar rutas redistribuidas desde el IGP.

Cuando un router es configurado para redistribuir información de enrutamiento desde un IGP a través de BGP, las rutas deben pasar exitosamente cualquier filtro que sea aplicado a la redistribución antes de que una ruta sea inyectada en la tabla BGP.

Configure un *Route-Map* para filtrar las rutas redistribuidas desde el enrutamiento RIPv2 dentro de BGP. Sólo las redes del espacio de direccionamiento asignado al AS 100 para ser publicado (100.128.0.0/17), deben ser insertadas en la tabla BGP del router AS1EDGE.

Para llevar a cabo esta tarea, deshabilite la redistribución ya implementada utilizando la forma **no** del comando **redistribute**, posteriormente configure el *Route-Map* solicitado y vuelva a habilitar la redistribución haciendo uso del comando:

**Redistribute***protocol***route-map***route-map-name*

Pasos para realizarlo:

1. Se crea una lista de prefijo en el router AS1EDGE así:
    a. AS1EDGE(config)#ip prefix-list FilterRIPAS100 seq 5 permit 100.128.0.0/17
2. Se crea un Route Map de la siguiente manera:
    a. AS1EDGE(config)#route-map MapRIPFilter permit 10
    b. AS1EDGE(config)#match ip address prefix-list FilterRIPAS100
    c. AS1EDGE(config-router)#redistribute rip route-map MapRIPFIlter

Una vez ejecutados los comandos anteriores en el router AS1EDGE (posteriores al deshabilitado de la redistribución RIP) BGP solamente realizará la redistribución de las rutas aprendidas mediante RIPv2 pero que se encuentren solamente dentro de la subredes especificadas mediante la lista de prefijo, es decir que el bloque de subredes 172.16.0.0/20 no será anunciado desde el router AS1EDGE mediante BGP.

**Consulte y analice:**

¿Qué beneficios o consecuencias trae la implementación de filtros en la redistribución de rutas desde un IGP hacia BGP?

_____

_____

_____

_____

**Paso 2:** Configurar *Route-Map* para filtrar rutas.

Opcionalmente, se pueden aplicar *filter-lists*, *prefix-lists* y *Route-Maps* para filtrar información ya sea entrante o saliente, o cualquier combinación posible de ambas. Los filtros de entrada deben permitir las rutas recibidas desde un vecino antes que estas sean insertadas dentro de la tabla BGP. Las rutas salientes deben pasar por los filtros de salida antes de ser transmitidas al vecino BGP.

Deshabilite los filtros de rutas entrantes desde o salientes hacia vecinos, en el proceso BGP del router AS1EDGE.Configure un *Route-Map* para filtrar rutas entrantes desde el AS 200 y el AS 300, el cual sólo permita la entrada de rutas estáticas predeterminadas (o ruta por defecto), y que a la vez establezca un valor ***weight*** de 150 para las rutas entrantes a través el enlace primario (AS 200), y un valor ***weight*** de 100 para las rutas entrantes a través del enlace secundario (AS 300). Posteriormente, configure una ruta estática predeterminada (o ruta por defecto) en cada uno de los routers: AS2EDGE1 y AS3EDGE1, y anúncielas sobre BGP manualmente utilizando el comando ***network***.

Pasos para realizarlo:

1. Se crea una lista de prefijo en el router AS1EDGE así:
   **a. AS1EDGE(config)#**ip prefix-list RoutesISPs seq 5 permit 0.0.0.0/0
2. Se crea un filtro de AS-Path así:
   **a. AS1EDGE(config)#**ip as-path access-list 10 permit _200$
3. Se crea un Route Map de la siguiente manera:
   **a. AS1EDGE(config)#**route-map MapISPsFilter permit 10
   **b. AS1EDGE(config)#**match ip address prefix-list RoutesISPs
   **c. AS1EDGE(config)#**match as-path 10
   **d. AS1EDGE(config)#**set weight 150
   **e. AS1EDGE(config)#**route-map MapISPsFilter permit 20
   **f. AS1EDGE(config)#**match ip address prefix-list RoutesISPs
   **g. AS1EDGE(config)#**set weight 100
   **h. AS1EDGE(config-router)#**neighbor 209.128.0.2 route-map MapISPsFilter in
   **i. AS1EDGE(config-router)#**neighbor 209.128.0.6 route-map MapISPsFilter in

Consulte y analice:

¿Cuál es el resultado de implementar dos valores diferentes de ***weight*** dependiendo del origen de las rutas?

_____
_____
_____
_____
_____
_____

Configure un *Route-Map* para filtrar rutas salientes hacia el AS 200 y el AS 300, el cual sólo permita la salida de rutas localmente originadas.

Pasos para realizarlo:

1. Se crea un filtro de AS-Path así:
   **a. AS1EDGE(config)#**ip as-path access-list 50 permit ^$
2. Se crea un Route Map de la siguiente manera:
   **a. AS1EDGE(config)#**route-map MapLocalFilter permit 10
   **b. AS1EDGE(config)#**match as-path 50
   **c. AS1EDGE(config-router)#**neighbor 209.128.0.2 route-map MapLocalFilter out
   **d. AS1EDGE(config-router)#**neighbor 209.128.0.6 route-map MapLocalFilter out

Por último, aplique los *Route-Map* a los vecinos utilizando el comando:

**Neighbor***neighbor-ip-address***route-map***route-map-name* {**in** | **out**}

De ser posible, reutilice listas de acceso y listas de prefijo ya existentes para realizar estas tareas.

**Paso 3:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

¿Es posible realizar un ping desde la interfaz *Loopback 1* del router AS2BR a cada una de las interfaces directamente conectadas a las LAN del router AS1R1? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 1* del router AS2BR a cada una de las interfaces directamente conectadas a las LAN del router AS1R2? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 1* del router AS2BR a cada una de las interfaces directamente conectadas a las LAN del router AS1R3? SI __ NO ___

Verifique la tabla BGP en el router AS1EDGE con el comando:

**AS1EDGE#**show ip bgp
Verifique la tabla BGP que tiene aplicado el route-map con el comando:
**AS1EDGE#**show ip bgp route-map **<nombre-route-map>**

Verifique que las tablas  BGP entregadas por ambos comandos presentan diferencias a nivel de los registros arrojados.

# CAPÍTULO CUATRO

## Índice laboratorio N° 4



## Índice de Figuras



## Índice de Tablas

# 4. LABORATORIO N° 4 - SELECCIÓN DE RUTA USANDO ATRIBUTOS

## 4.1 INTRODUCCION

Al igual que los protocolos de Gateway interior, BGP cuenta con un mecanismo que le permite medir la "distancia" entre dos puntos en una red determinada. Cada ruta aprendida a través de BGP tiene un conjunto de parámetros asociados, denominados **atributos de ruta BGP**. Este conjunto de valores permiten a BGP determinar que ruta usar cuando existen múltiples rutas hacia la misma red de destino.

El grado de elegibilidad de una ruta está ligado a una serie de criterios que sirven para determinar cuál es la mejor ruta. Los atributos asociados a cada ruta tienen valores predeterminados susceptibles de ser modificados lo que permite influenciar el proceso de selección de ruta de acuerdo a criterios de diseño, políticas de enrutamiento o acuerdos comerciales establecidos entre el cliente y el proveedor de servicio de internet (ISP) u otros ASs.

Este laboratorio está orientado a comprender como operan los diversos atributos de ruta BGP incluyendo *weight*, *local preference*, *AS-pathprepending*, *multi-exitdiscriminator* (*MED*) y *BGP communities*, y como modificar sus valores por defecto para influir en el proceso de selección de ruta BGP con el ánimo de satisfacer las políticas de enrutamiento establecidas.

En la topología se muestran los clientes A y B conectados entre sí y a su vez conectados al cliente C (una compañía que ofrece servicios de misión crítica a través de internet), a través de dos proveedores de servicio de internet independientes (ISPs X y Y). Los clientes A y B

están conectados a ambos ISPs, mientras que el cliente C tiene dos conexiones independientes con el ISP Y. Para los clientes A y B el ISP X es el ISP principal y el ISP Y actúa como ISP de respaldo, por lo tanto en condiciones normales, el tráfico entre los clientes A y B hacia el cliente C debe fluir a través del ISP X atravesando la infraestructura del ISP Y.

## 4.2 OBJETIVOS

- Configurar BGP para influir en la selección de ruta mediante el uso del atributo weight en un escenario de red que debe soportar la conexión a múltiples ISPs.
- Usar el atributo local preference para influir en la selección de ruta en un escenario de red que debe soportar la conexión a múltiples ISPs.
- Usar el mecanismoAS-pathprepending para influir en la selección de ruta de retorno seleccionada por el sistema autónomo vecino en un escenario de red que debe soportar la conexión a múltiples ISPs.
- Usar el atributo MED para influir en la selección de ruta en un escenario de red que debe soportar la conexión a múltiples ISPs.
- Usar el atributo community BGP para influir en la selección de ruta en un escenario de red que debe soportar la conexión a múltiples ISPs.

## 4.3 DIAGRAMA DE TOPOLOGIA

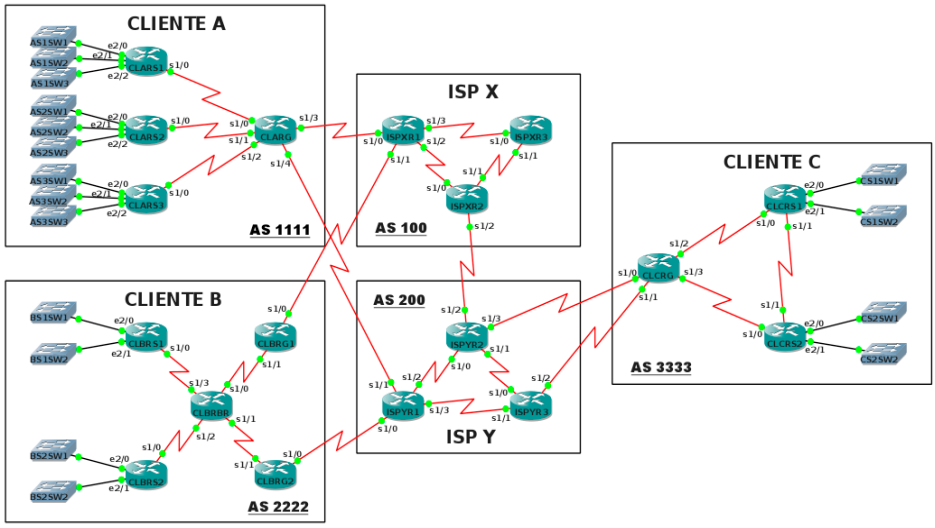


***Figura 4.1.*** Topología Selección de Ruta Usando Atributos

## 4.4 TABLAS DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| ISPX-R1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback 0 | | |
| ISPX-R2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Loopback 0 | | |
| ISPX-R3 | Serial1/0 | | |
| | Serial1/1 | | |
| | Loopback 0 | | |

Tabla 4.1. Selección de Ruta Usando Atributos [ISP X]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| ISPY-R1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback 0 | | |
| ISPY-R2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback 0 | | |
| ISPY-R3 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Loopback 0 | | |

Tabla 4.2. Selección de Ruta Usando Atributos [ISP Y]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CLA-RG | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Serial1/4 | | |
| | Loopback 0 | | |
| CLA-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |
| | Loopback 0 | | |
| CLA-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |
| | Loopback 0 | | |
| CLA-RS3 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |
| | Loopback 0 | | |

Tabla 4.3. Selección de Ruta Usando Atributos [CLIENTE A]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CLB-RG1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Loopback 0 | | |
| CLB-RG2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Loopback 0 | | |
| CLB-RBR | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback 0 | | |
| CLB-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Loopback 0 | | |
| CLB-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Loopback 0 | | |

Tabla 4.4. Selección de Ruta Usando Atributos [CLIENTE B]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CLC-RG | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback 0 | | |
| CLC-RS1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Loopback 0 | | |
| CLC-RS2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Loopback 0 | | |

Tabla 4.5. Selección de Ruta Usando Atributos [CLIENTE C]

# 4.5 DESCRIPCIÓN DE LA ACTIVIDAD

## TAREA 1: Diseñar y documentar un esquema de direccionamiento

**Paso 1:** Diseñe un esquema de direccionamiento.

Utilice la topología mostrada previamente y diseñe el esquema de direccionamiento con base en los siguientes requisitos:

- El espacio de dirección para la red del cliente A es 11.1.0.0/16. Deberá asignar a cada router de sucursal (CLA-RS1, CLA-RS2 y CLA-RS3) un espacio de dirección según estos requisitos.
  - CLA-RS1 necesita espacio para 16 000 hosts _____
  - CLA-RS2 necesita espacio para 8000 hosts _____
  - CLA-RS3 necesita espacio para 4000 hosts _____

- Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router. Divida el espacio de dirección para cada router de sucursal en tres subredes iguales. Registre las subredes en la siguientes tablas:

| **Router** | **Interfaz** | **Número de subred** | **Dirección de subred** | **Máscara de subred** |
|---|---|---|---|---|
| CLA-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

| **Router** | **Interfaz** | **Número de subred** | **Dirección de subred** | **Máscara de subred** |
|---|---|---|---|---|
| CLA-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLA-RS3 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

- Para las WAN en la red del cliente A, realice una conexión con una subred en la dirección 10.1.128.0/28. La conexión CLA-RS1 a CLA-RG utiliza la primera subred, la conexión CLA-RS2 a CLA-RG utiliza la segunda y la conexión CLA-RS3 a CLA-RG la tercera. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLA-RS1 <> CLA-RG | 0 | | |
| CLA-RS2 <> CLA-RG | 1 | | |
| CLA-RS3 <> CLA-RG | 2 | | |

- El espacio de dirección para la red del cliente B es 12.1.0.0/16. Deberá asignar a cada router de sucursal (CLB-S1, CLB-S2) un espacio de dirección según estos requisitos.

    - CLB-S1 necesita espacio para 16000 hosts _____
    - CLB-S2 necesita espacio para 8000 hosts _____

- Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router. Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLB-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLB-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

- Para las WAN en la red del cliente B, realice una conexión con una subred en la dirección 10.2.128.0/27. La conexión CLB-RS1 a CLB-RBR utiliza la primera subred, la conexión CLB-RS2 a CLB-RBR utiliza la segunda, la conexión CLB-RG1 a CLB-RBR utiliza la tercera, la conexión CLB-RG2 a CLA-RBR, la cuarta. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLB-RS1 <> CLB-RBR | 0 | | |
| CLB-RS2 <> CLB-RBR | 1 | | |
| CLB-RG1 <> CLB-RBR | 2 | | |
| CLB-RG2 <> CLB-RBR | 3 | | |

- El espacio de dirección para la red del cliente C es 13.1.0.0/16. Deberá asignar a cada router de sucursal (CLC-RS1, CLC-RS2) un espacio de dirección según estos requisitos.

    - CLC-RS1 necesita espacio para 1000 hosts _____
    - CLC-RS2 necesita espacio para 500 hosts _____

- Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router. Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLC-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLC-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

- Para las WAN en la red del cliente C, realice una conexión con una subred en la dirección 10.3.128.0/28. La conexión CLC-RS1 a CLC-RG utiliza la primera subred y la conexión CLC-RS2 a CLC-RG, la segunda, y la conexión CLC-RS1 a CLC-RS2 utiliza la tercera. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLC-RS1 <> CLC-RG | 0 | | |
| CLC-RS2 <> CLC-RG | 1 | | |
| CLC-RS1 <> CLC-RS2 | 2 | | |

- Para las WAN en la red del ISP X, realice una conexión con una subred en la dirección 172.16.0.0/28. La conexión ISPX-R1 a ISPX-R2 utiliza la primera subred, la conexión ISPX-R1 a ISPX-R3 utiliza la segunda, la conexión ISPX-R2 a ISPX-R3 utiliza la tercera. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| ISPX-R1 <> ISPX-R2 | 0 | | |
| ISPX-R1 <> ISPX-R3 | 1 | | |
| ISPX-R2 <> ISPX-R3 | 2 | | |

- Para las WAN en la red del ISP Y, realice una conexión con una subred en la dirección 172.17.0.0/28. La conexión ISPY-R1 a ISPY-R2 utiliza la primera subred, la conexión ISPY-R1 a ISPY-R3 utiliza la segunda, la conexión ISPY-R2 a ISPY-R3 utiliza la tercera. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| ISPY-R1 <> ISPY-R2 | 0 | | |
| ISPY-R1 <> ISPY-R3 | 1 | | |
| ISPY-R2 <> ISPY-R3 | 2 | | |

- Para las WAN que conectan los clientes A, B y C a los proveedores de servicio, utilice la subred en la dirección 192.168.0.0/27.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLA-RG <> ISPX-R1 | 0 | | |
| CLB-G1 <> ISPX-R1 | 1 | | |
| CLA-RG <> ISPY-R1 | 2 | | |
| CLB-G2 <> ISPY-R1 | 3 | | |
| CLC-RG <> ISPY-R2 | 4 | | |
| CLC-RG <> ISPY-R3 | 5 | | |
| ISPX-R2 <> ISPY-R2 | 6 | | |

**Paso 2:** Documente el esquema de direccionamiento.

Documente las direcciones IP y máscaras de subred. Para las sucursales asigne la primera dirección IP a la interfaz del router.

En los enlaces WAN entre el cliente A, B y C y los ISPs utilice la primera dirección IP para los routers de borde de ambos ISPs.

## TAREA 2: Preparación básica de la red

**Paso 1:** Conecte una red que sea similar a la del diagrama de topología.

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en el gráfico.

**Paso 2:** Configuración básica de los enrutadores.

Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautasgenerales (utilice como contraseña la palabra *"nyquist"*):

1. Configure el nombre de host del router.
2. Configure una contraseña de modo EXEC privilegiado.
3. Configure un mensaje del día.

4. Configure una contraseña para las conexiones de la consola.
5. Configure una contraseña para las conexiones de VTY.

## TAREA 3: Configuración del enrutamiento dinámico

**Paso 1:** Configurar el enrutamiento OSPF en ambos ISPs.

Configure el enrutamiento OSPF (identificador de proceso número 1) en cada router de cada ISP. Use el número 10 como identificador de área para OSPF.

**Paso 2:** Configurar el enrutamiento EIGRP en los cliente A y B.

Configure todos los dispositivos con un enrutamiento EIGRP en la red de los clientes A y B. En la configuración, asegúrese de:

- Desactivar la sumarización automática.
- Detener las actualizaciones de enrutamiento en las interfaces que no estén conectadas a los vecinos de EIGRP.

**Paso 3:** Configurar el enrutamiento RIPv2 en el cliente C.

Configure todos los routers en la red del cliente C con RIPv2 como protocolo de enrutamiento dinámico.

- Deshabilite la sumarización automática.
- Deshabilite las actualizaciones RIP en las interfaces que no estén conectadas a los vecinos de RIPv2.

## TAREA 4: Establecer mallas completas de sesiones IBGP en cada AS

Utilice el siguiente comando en el modo de configuración del router para crear mallas completas de sesiones IBGP al interior de los Clientes A, B y C y al interior de ambos ISPs:

**neighbor***ip address* **remote-as** *as-number*

Asegúrese de utilizar interfaces *Loopback* para establecer las sesiones IBGP mediante el siguiente comando de configuración del router:

**neighbor***ip-address* **update-source** *interface*

**Paso 1:** Establezca una malla completa de sesiones IBGP en el ISP X.

Establezca sesiones IBGP entre todos los routers de borde del ISP X.
**Paso 2:** Establezca una malla completa de sesiones IBGP en el ISP Y.

Establezca sesiones IBGP entre todos los routers de borde del ISP Y.

**Paso 3:** Establezca una malla completa de sesiones IBGP en el cliente A.

- Desde el router de borde CLA-RG establezca sesiones IBGP a los demás routers del AS.
- Desde los routers de sucursal CLA-RS1, CLA-RS2 y CLA-RS3 establezca sesiones IBGP con el router frontera CLA-RG.

**Paso 4:** Establezca una malla completa de sesiones IBGP en el cliente B.

- Desde los routers de borde CLB-RG1 y CLB-RG2 establezca sesiones IBGP a los demás routers del AS, así como sesiones entre sí.
- Desde los routers CLB-RS1, CLB-RS2 y CLB-RBR establezca sesiones IBGP con los routers frontera CLB-RG1 y CLB-RG2.

**Paso 5:** Establezca una malla completa de sesiones IBGP en el cliente C.

- Desde el router de borde CLC-RG establezca sesiones IBGP a los demás routers del AS.
- Desde los routers de sucursal CLC-RS1 y CLC-RS2 establezca sesiones IBGP con el router frontera CLC-RG.

## TAREA 5: Establecer sesiones EBGP entre ambos ISPs y los clientes A, B y C

Establezca sesiones EBGP entre los routers de borde de cada cliente con los routers frontera de cada ISP así como entre ambos ISPs tal como lo muestra el diagrama de topología.

Utilice el comando **neighbor***ipaddress***remote-as** *as-number*en el modo de configuración del router.

## TAREA 6: Anunciar redes

**Paso 1:** Anuncie las redes al interior de la red del cliente A.

Anuncie las redes necesarias a través del comando de configuración de router **network**sin la opción **mask.**
Enuncie las redes que publicará a través del comando **network**

- Red1_____

¿Es necesario crear rutas predeterminadas que apunten a la interfaz *null0*?, ¿Por qué?

_____

_____

**Paso 2:** Anuncie las redes al interior de la red del cliente B.

Redistribuya las rutas desde el IGP a BGP y a través de un mapa de ruta establezca un filtro que deniegue las direcciones privadas de ruta y cambie el código origen de las rutas redistribuidas a **internal (i)**.

Utilice el siguiente comando en el modo de configuración del router:

Formato general
**redistribute***protocol* [*process-ID*] {**level-1 | level-1-2 | level-2**} [**metric** *metric-value*][**match** {**internal | external 1 | external 2**}] [tag *tag-value*][**route-map** *map-tag*][**weight** *weight*] [**subnets**]

Formato a aplicar
**redistribute**<protocol>**route-map**<route-map-name>

Se creó en el router CLBRG1 y en el router CLBRG2 el siguiente prefix-list y el siguiente route-map, así:

**Router(config)#**ip prefix-list FiltroIGPseq 5 permit 12.1.0.0/16 le 20
**Router(config)#**route-map MapIGP permit 10
**Router(config-route-map)#**match ip address prefix-list FiltroIGP
**Router(config-route-map)#**set origin igp
**Router(config-router)#**redistribute eigrp 10 route-map MapIGP

**Paso 3:** Anuncie las redes al interior de la red del cliente C.

Haga un resumen de ruta para las redes que desea publicar.

Enuncie las redes que publicará a través del resumen de ruta

- Red1 _____ mascara de subred _____
- Red2 _____ mascara de subred_____

¿Qué condiciones deben cumplir estas redes para ser anunciadas como resúmenes de ruta?

_____

_____

_____

_____

Utilice el siguiente comando en el modo de configuración del router:

**aggregate-address***address mask* [**as-set**][**suppress-map** *map-name*][**advertise-map** *map-name*][**attribute-map** *map-name*]

Es necesario asegurar que sólo se anuncie el resumen de red y no las redes individuales. ¿Qué palabra clave debe agregar al comando para garantizar este requerimiento?

Nota: En el primer paso se anuncian solamente los resumenes de ruta mediante el comando redistribute static y creando dos rutas exactas para cada subred a la interfaz null 0. En el segundo paso simplemente se realiza un aggregate-address para que sólo se anuncie la red sumarizada que contiene a las dos subredes del paso anterior (es decir 13.1.0.0 255.255.248.0) y con el parametro summary-only al final del comando aggregate-address.

## TAREA 7: Garantizar la resolución de direcciones de siguiente salto (Next-Hop)

Para llevar a cabo esta tarea tiene tres funciones que puede utilizar de acuerdo a su criterio:

- Asegúrese que todos los routers de borde que contienen sesiones EBGP redistribuyan las subredes conectadas en el IGP utilizando el comando redistributeconnected en el modo de configuración del protocolo de enrutamiento (no anuncie esta red médiate el comando network).

- Incluya la subred en la que se está ejecutando la sesión EBGP en la configuración del IGP usando el comando network asegurándose que el router de borde no intercambie información de enrutamiento IGP con el router de borde del otro AS configurando la interfaz como interface pasiva.

- Utilice el comando next-hop-self en el modo de configuración del router.

## TAREA 8: Definir filtros

**Paso 1:** Asegúrese que ninguno de los clientes actúe como un AS de transporte para ambos ISPs.
Debe evitar que los clientes A, B y C actúen como sistemas autónomos de transporte para ambos ISPs.
Defina la expresión regular que permita anunciar sólo las redes de origen local de cada cliente. _____

Utilice los siguientes comandos:

- ip as-path access-list access-list-number {permit|deny} as-regular-expression
- neighbor {ip-address|peer-group-name} filter-list access-list-number {in|out}

**Paso 2:** Filtre el tráfico proveniente de los clientes A, B y C en ambos proveedores de servicio.

Tanto en el ISP X como en el ISP Y establezca filtros que denieguen cualquier dirección IP privada y permitan solo el bloque de direcciones público asignado a cada cliente.

Utilice los siguientes comandos de configuración:

- ip prefix-list list-name [seqseq-value] {permit|deny} network/len[gege-value] [le le-value]
- neighbor {ip-address|peer-group-name} prefix-list prefix-listname{in|out}

**Paso 3:** En ambos ISPs permita el tráfico sólo de los ASs vecinos conectados directamente.

Establezca una lista de acceso *AS-path* que permita solo el tráfico proveniente de los AS vecinos conectados directamente.

Establezca la expresión regular que coincida con cualquier vecino conectado directamente:

_____

_____

**Nota:** Para mayor comodidad puede establecer estos filtros a través de mapas de ruta.

## TAREA 9: Seleccione la ruta óptima para el flujo del tráfico saliente

Cuando existen conexiones a múltiples ISPs, es importante garantizar que BGP seleccione la mejor ruta a usar para el flujo del tráfico de salida de modo que se satisfaga las políticas administrativas establecidas. En este caso para los clientes A y B el tráfico de salida desde cada cliente debe fluir hacia el enlace de alta velocidad de 2 Mbps que los conecta con el ISP X y el enlace de baja velocidad que conecta los clientes con el ISP Y debe usarse solo cuando falle el enlace principal. Para las conexiones entre el cliente C y el ISP Y el flujo de información debe fluir a través del enlace que conecta el router ISPY-R3 al router frontera de este cliente. El enlace adicional debe usarse solo para propósitos de respaldo.

Utilice los siguientes comandos en el modo de configuración del router:

- neighbor {ip-address|peer-group-name} weight weight
- bgpdefaulf local-preference preference

Si requiere el uso de mapas de ruta utilice los siguientes comandos ***set*** para modificar los valores *weightylocal preference*:

- set weight weight
- set local-preference value

**Paso 1:** Asegúrese que el tráfico de salida del cliente A fluya a través del enlace de 2 Mbps que lo conecta al ISP X.

Use el atributo **weight**para satisfacer este requerimiento.

El Atributo *weight* es el primer parámetro tomado en consideración en el proceso de selección de ruta. Cuando existen múltiples rutas hacia una red IP de destino, el proceso BGP elegirá la ruta con el mayor valor *weight*. Este atributo es de importancia a nivel local, lo que constituye una política de enrutamiento local para el router, ya que este valor no se propaga a los demás routers vecinos. El atributo *weight*tiene un valor por defecto de 0.

**Paso 2:** Asegúrese que el tráfico de salida del cliente B fluya a través del enlace de 2 Mbps que lo conecta al ISP X.

Use el atributo *weight* o el atributo *local preference* para satisfacer este requerimiento.

El Atributo *local preference* es el segundo parámetro tomado en consideración en el proceso de selección de ruta. Cuando existen múltiples rutas hacia una red IP de destino, el proceso BGP elegirá la ruta con el mayor valor *local preference*. Este atributo constituye una política de enrutamiento global para el AS, ya que este valor se propaga desde los routers de borde del AS a los demás routers vecinos a través de sesiones IBGP. El atributo *local preference* tiene un valor por defecto de 100. Este atributo se toma en consideración solo cuando las rutas examinadas tienen el mismo valor *weight*. El router aplicará este valor a las rutas originadas localmente y a las actualizaciones provenientes de ASs vecinos. Este valor será eliminado en las actualizaciones de salida EBGP.

¿En este caso específico por qué constituye una ventaja utilizar el atributo *local preference* para garantizar que el tráfico de salida del cliente B fluya a través del enlace de 2 Mbps que lo conecta al ISP X en lugar del atributo *weight*?

**Paso 3:** Asegúrese que el tráfico de salida del cliente C fluya a través del enlace de 2 Mbps que lo conecta al ISP Y.

Use el atributo *local preference* para satisfacer este requerimiento.

¿Es necesario utilizar un mapa de ruta? ¿Por qué?

**Nota importante:** Cuando se usan los comandos tipo <match ip> dentro de un RouteMap, estos sólo pueden ser usados para que posteriormente el RouteMap sea aplicado en el sentido de salida. Si se usan estos comandos tipo match dentro de un RouteMap y posteriormente se aplica con sentido de entrada, el IOS no permitirá aplicarlo.

## TAREA 10: Seleccione la ruta óptima para el flujo del tráfico entrante

Cuando existen conexiones a múltiples ISPs, además de garantizar que BGP seleccione la mejor ruta a usar para el flujo del tráfico de salida también es importante que la ruta de retorno seleccionada sea la ruta óptima y satisfaga las políticas de enrutamiento definidas. En este caso el tráfico de entrada desde el ISP X hacia los clientes A y B debe fluir por el enlace de alta velocidad de 2 Mbps que los conecta, el enlace de baja velocidad que los conecta con el ISP Y debe usarse solo cuando falle el enlace principal.

**Nota:** Configurar la ruta preferida solo para el tráfico de salida y no para el tráfico de entrada podría probablemente dar como resultado un *flujo de tráfico asimétrico.*

¿A que se denomina flujo de tráfico asimétrico?

El tráfico entrante para los clientes A, B y C es el resultado del proceso de selección de ruta para el tráfico de salida tanto en el ISP X como en el ISP Y. Asuma que no tiene control sobre la configuración de los routers al interior de ambos ISPs.
¿Bajo estas circunstancias es posible influenciar al flujo del tráfico de regreso en los ISP desde los clientes mediante la configuración de los parámetros *weight* y *local preference* de manera que el flujo de entrada a los clientes fluya a través del enlace de alta velocidad que conecta al

ISP X con los clientes, y que conmute al enlace de 64 kbps en caso de producirse una falla en el enlace principal? ¿Por qué?

¿Es posible bajo las circunstancias establecidas (no hay control sobre la configuración de los routers al interior de ambos ISPs) que los clientes A, B y C hagan peticiones a ambos ISPs solicitando la modificación de sus políticas administrativas con el fin de satisfacer su propia política de enrutamiento interna? ¿Por qué?

¿Qué alternativas tiene para influir en el proceso de selección de ruta en ambos ISP para que satisfagan la política de enrutamiento de los diferentes clientes?

**Paso 1:** Asegúrese que el tráfico entrante para el cliente A fluya a través del enlace de alta velocidad que lo conecta al ISP X.

"La información de AS-PATH se manipula a menudo para afectar el comportamiento del enrutamiento entre dominios. Dado que BGP prefiere una ruta AS-PATH más corta antes que una más larga, los operadores de red están tentados a modificar la información de ruta incluyendo entradas AS-PATH falsas que incrementarían la longitud de la ruta para influir o disuadir la trayectoria del tráfico. La implementación de Cisco permite a un usuario añadir los números de AS al principio de un AS-PATH para alargar la longitud de la ruta."[10]
Para lograr este objetivo modifique la longitud del AS-path de forma que el tráfico de entrada hacia el cliente A fluya a través del enlace que lo conecta al ISP de respaldo solo si se presenta una falla en el enlace principal.

Utilice el siguiente comando **set** a través de un mapa de ruta para modificar la longitud del atributo *AS-Path*:

10 HALABI, Sam; MCPHERSON, Danny. Arquitectura de enrutamiento en Internet. Segunda Edición. Pearson Education. España. 2001. p. 166.

**set as-path prepend** *as-number*[*as-number…*]

¿A través de qué enlace el cliente A debe enviar el atributo AS-path con la longitud modificada?

¿Cuál debe ser la longitud mínima del atributo AS-path modificado para lograr que el tráfico de entrada para el cliente A fluya a través del enlace principal?

¿Señale que tipo de problemas se pueden presentar si el router que modifica la longitud del atributo AS-path introduce un número AS diferente al número de AS al que pertenece?

Mediante los comandos *show* verifique que el tráfico de entrada para el Cliente A fluye de la forma esperada.

¿A través de qué enlace está fluyendo el tráfico de entrada en el cliente A? ¿Por qué?

Modifique el filtro y establezca la expresión regular correcta que permita el uso de la función AS-pathprepending _Si se estaba usando **(^1111$) cambiarla por (_1111$)_**.

**Paso 2:** Asegúrese que el trafico entrante para el cliente B fluya a través del enlace de alta velocidad que lo conecta al ISP X.
Para lograr este objetivo modifique la longitud del AS-path de forma que el tráfico de entrada hacia el cliente B fluya a través del enlace que lo conecta al ISP de respaldo solo si se presenta una falla en el enlace principal.

Se debe implementar de la siguiente manera, similar a lo implementado para el Cliente A. Se debe ejecutar sobre el router que conecta al ISP que se quiere usar como respaldo para el flujo de tráfico de regreso.

**CLBRG2(config)#route-map MapPrependY permit 10**
**CLBRG2(config-route-map)#set as-path prepend 2222 2222**
**CLBRG2(config-route-map)#exit**
**CLBRG2(config)#router bgp 2222**
**CLBRG2(config-router)#neighbor 192.168.0.13 route-map MapPrependY out**

**Paso 3:** Asegúrese que el trafico entrante para el cliente C fluya a través del enlace de alta velocidad que lo conecta al ISP Y.

Use el atributo *Multi-ExitDiscriminator (MED)* para satisfacer este requerimiento.

El Atributo *Multi-ExitDiscriminator (MED)* es un atributo opcional no transitivo. Este atributo es útil cuando existen múltiples puntos de entrada en un AS. Si existen múltiples enlaces que conectan dos ASs adyacentes, se puede usar este atributo para informarle al otro AS cuál de los enlaces usar para llegar a un punto determinado al interior de la red. El valor por defecto de este atributo es 0. El proceso BGP elegirá la ruta con el menor valor. Este atributo se toma en consideración solo cuando las rutas examinadas tienen el mismo valor para los parámetros *weight, local preference, AS-path* y código origen. Este atributo no es propagado fuera del AS receptor.[11]

Utilice el siguiente comando ***set*** a través de un mapa de ruta para modificar el valor *MED* predeterminado:

**set metric** *value*

Se debe implementar en el router CLCRG del AS 3333 dos mapas de rutas, aplicarlos a cada vecino de la siguiente manera:

**CLCRG(config)#route-map MapMED permit 10**
**CLCRG(config-route-map)#set metric 10**
**CLCRG(config)#route-map MapMEDno permit 10**
**CLCRG(config-route-map)#set metric 20**
**CLCRG(config-router)#neighbor 192.168.0.17 route-map MapMEDno out**
**CLCRG(config-router)#neighbor 192.168.0.21 route-map MapMED out**

Antes de implementar estos mapas de ruta, las rutas para el segmento de red 13.1.0.0/22 y

11 Cisco Systems Learning. Configuring BGP on Cisco Routers. Volume 2. Version 3.2. Estados Unidos. 2005. p. 73.

13.1.4.0/23 en el AS 200 del operador Y se presentaban así:

Para el router ASPYR1 los siguientes saltos para ambas rutas apuntaban a la dirección IP 192.168.0.18, ya que el peso, la preferencia local y el AS-Path eran idénticos, teniendo como criterio de desempate el router ID, que en este caso será elegido a través del router ID más bajo que corresponde a la ruta anunciada por el router ISPYR2 que posee un router ID 2.2.2.2 mientras que para ISPYR3 se cuenta con un router ID de 2.2.2.3.

Para el router ISPYR2 los siguientes saltos para ambas rutas apuntaban a 192.168.0.18, ya que es preferible una ruta aprendida por un peer EBGP que por un IBGP, si los paquetes deben abandonar el AS deben hacerlo de la forma más rápida (directo al router del AS vecino y no a través del router ISPYR3 para después pasar al router del AS vecino).

Para el router ISPYR3 aplica el mismo concepto que para el router ISPYR2, es preferible una ruta aprendida por un peer EBGP que por un peer IBGP.

Después de implementar los mapas de ruta en el router CLCRG del AS 3333, todos los enrutadores del AS 200 correspondiente al ISP Y, presentan como siguiente salto en la ruta para las redes 13.1.0.0/22 y 13.1.4.0/23 a la dirección IP 192.168.0.22.

## TAREA 11: Seleccione la ruta óptima para el flujo del tráfico entrante mediante el atributo community BGP

"En el contexto de BGP, una comunidad es un grupo de destinos que comparten algún tipo de propiedad común. Una comunidad no está restringida a una red o a un sistema autónomo; no tiene límites físicos. Las comunidades son utilizadas para simplificar las políticas de enrutamiento mediante la identificación de rutas basadas en una propiedad lógica en lugar de un prefijo IP o en un número de SA. Un portavoz BGP puede utilizar este atributo en conjunción con otros para controlar las rutas que se aceptarán, preferirán y transmitirán a otros vecinos BGP."[12]

12 HALABI, Sam; MCPHERSON, Danny. Arquitectura de enrutamiento en Internet. Segunda Edición. Pearson Education. España. 2001. p. 159.

Utilice los siguientes comandos:

**route-map***name*
**match** *condition*
**set community** *value [value…][additive]*
**neighbor** *ip-address* **send-community**
**ip community-list** {*standard-list-number* | *expanded-list-number [regular-expression]* | {**extandard**| **expanded**} *community-list-name*} {**permit** | **deny**} {*community-number* | *regular-expression}*

¿Qué tipo de atributo BGP es el atributo *community*?

¿Qué significado tiene el primer número que conforma este atributo?

¿Qué significado tiene el segundo número que conforma este atributo?

Ambos proveedores publicaron una lista que muestra una lista de *communities* y los objetivos que cumplen.

| Objetivo | Valor Community |
|---|---|
| Establecer local preference50 | 300:11 |
| Establecer local preference150 | 300:12 |
| Anteponer AS-pathuna vez cuando se envíe la red a vecinos externos | 300:13 |
| Anteponer AS-path dos veces cuando se envíe la red a vecinos externos | 300:14 |
| Anteponer AS-path tres veces cuando se envíe la red a vecinos externos | 300:15 |
| Establecer el MED a 100 | 300:16 |

***Tabla 4.6.*** Selección de Rutas Usando Atributos [Communities ISP X]

| Objetivo | Valor Community |
|---|---|
| Establecer local preference80 | 400:21 |
| Establecer local preference180 | 400:22 |
| Anteponer AS-pathuna vez cuando se envíe la red a vecinos externos | 400:23 |
| Anteponer AS-path dos veces cuando se envíe la red a vecinos externos | 400:24 |
| Anteponer AS-path dos tres cuando se envíe la red a vecinos externos | 400:25 |
| Establecer el MED a 120 | 400:26 |
| Establecer el MED a 50 | 400:27 |

Tabla 4.7. Selección de Rutas Usando Atributos [Communities ISP Y]

**Paso 1:** Elimine las configuraciones previas que garantizan que el fluyo del tráfico fluya desde los ISP hacia los clientes a través del enlace de alta velocidad.
BGP ofrece un poderoso mecanismo denominado *community* que permite influir sobre otros ASs para seleccionar la ruta de retorno adecuada para el flujo de tráfico mediante el etiquetado de rutas.[13]

En la tarea anterior se seleccionó la ruta óptima para el flujo del tráfico entrante para los clientes A, B y C mediante la modificación de la longitud del atributo *AS-path* a través de la función *AS-pathprepending* y la configuración del atributo *MED*. En esta tarea se utilizara el atributo *community* para seleccionar la ruta de retorno adecuada, por tanto es necesario eliminar las configuraciones previas.

**Paso 2:** Establezca los filtros adecuados en ambos ISP para cumplir con las tablas mostradas previamente.

Cree los *community-list* y los mapas de ruta adecuados que reflejen los valores *communities* y sus objetivos asignados.

**Paso 3:** Asegúrese que el trafico entrante para el cliente A fluya a través del enlace de alta velocidad que lo conecta al ISP X.

Para lograr este objetivo etiquete las rutas con cualquiera de los valores *community* que modifican el atributo *local preference.*

13 Cisco Systems Learning.Configuring BGP on Cisco Routers.Volume 2. Version 3.2. Estados Unidos. 2005. p. 92.

**Paso 4:** Asegúrese que el trafico entrante para el cliente B fluya a través del enlace de alta velocidad que lo conecta al ISP X.

Para lograr este objetivo etiquete las rutas con cualquiera de los valores *community* que modifican la longitud del atributo *AS-path*.

**Paso 5:** Asegúrese que el trafico entrante para el cliente C fluya a través del enlace de alta velocidad que lo conecta al ISP Y.

Para lograr este objetivo etiquete las rutas con cualquiera de los valores *community* que modifican el atributo *MED*.

## TAREA 12: Verificar la completa conectividad entre todos los dispositivos de la topología

**Paso 1:** Pruebe la conectividad.

- Ahora debe tener conectividad de extremo a extremo. Utilice el ping para probar la conectividad a través de la red. ¿Cada router tiene respuesta al realizar un ping a todas las otras interfaces de cada router local y remoto del As? SI ___ NO ___
- Resuelva los problemas que se presenten hasta que los pings tengan éxito.

**Paso 2:** Examine la configuración**.**

Utilice los comandos de verificación para asegurarse de haber completado sus configuraciones.

# CAPÍTULO CINCO

# Índice laboratorio N° 5

# Índice de Figuras



# Índice de Tablas

# 5. LABORATORIO N° 5 - TIPOS DE CONECTIVIDAD ENTRE EL CLIENTE Y EL ISP

## 5.1. INTRODUCCION

Existen múltiples métodos de conexión entre un cliente y el proveedor de servicio de internet. Cada tipo de conexión requiere métodos diferentes para el intercambio de la información de enrutamiento así como diferentes esquemas de direccionamiento.

Cada una de estas conexiones está orienta a satisfacer los diferentes requerimientos que puede llegar a tener un cliente. De este modo el cliente debe escoger el tipo de conexión que mejor se acomode a su estructura organizacional para poder cumplir con sus objetivos corporativos, políticas administrativas y sus diferentes políticas de enrutamiento.

Este laboratorio muestra cada una de las diferentes formas de conexión desde un cliente a uno o más ISPs y las características de cada tipo de conexión física.

En la topología se muestran los clientes A, B, C, D y E conectados entre sí a través de dos proveedores de servicio de internet independientes (ISPs X y Y). El cliente A esta conectado únicamente al ISPX mediante un solo enlace, El cliente B tiene dos conexiones entre routers de borde independientes con el ISPX. El cliente C tiene dos conexiones independientes con el ISPX: estas conexiones se establecen desde el router de borde de este cliente hacia uno de

los routers de borde del ISP X. El cliente D tiene el mismo tipo de conexión que el cliente B y finalmente el cliente E tiene dos conexiones independientes a ambos ISPs.

En dichos escenarios se establecerán configuraciones *primary/backup* y *load sharing*.

## 5.2. OBJETIVOS

- Implementar conectividad con el cliente mediante el uso de enrutamiento estático en la red del proveedor de servicio.
- Implementar conectividad con el cliente a través de BGP estableciendo una configuración que soporte múltiples conexiones a un único ISP.
- Implementar conectividad con el cliente usando BGP en un escenario que soporte conexiones múltiples ISPs.

## 5.3. DIAGRAMA DE TOPOLOGIA

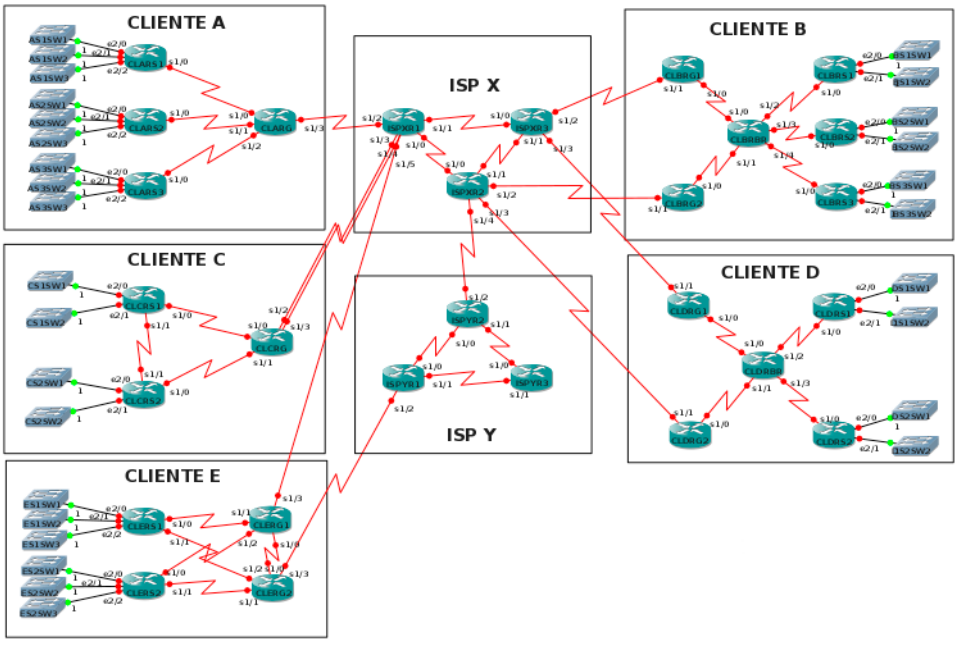


***Figura 5.1*** Topología Tipos de Conectividad Cliente-ISPs

## 5.4. TABLAS DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| ISPX-R1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Serial1/4 | | |
| | Serial1/5 | | |
| ISPX-R2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Serial1/4 | | |
| ISPX-R3 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |

Tabla 5.1.Tipos de Conectividad Cliente-ISPs [ISP X]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| ISPY-R1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| ISPY-R2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| ISPY-R3 | Serial1/0 | | |
| | Serial1/1 | | |

Tabla 5.2.Tipos de Conectividad Cliente-ISPs [ISP Y]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CLA-RG | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| CLA-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |
| CLA-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |
| CLA-RS3 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |

Tabla 5.3.Tipos de Conectividad Cliente-ISPs [CLIENTE A]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CLB-RG1 | Serial1/0 | | |
| | Serial1/1 | | |
| CLB-RG2 | Serial1/0 | | |
| | Serial1/1 | | |
| CLB-RBR | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Serial1/4 | | |
| CLB-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| CLB-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

| | | | |
|---|---|---|---|
| CLB-RS3 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 5.4.Tipos de Conectividad Cliente-ISPs [CLIENTE B]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CLC-RG | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| CLC-RS1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| CLC-RS2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 5.5. Tipos de Conectividad Cliente-ISPs [CLIENTE C]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CLD-RG1 | Serial1/0 | | |
| | Serial1/1 | | |
| CLD-RG2 | Serial1/0 | | |
| | Serial1/1 | | |
| CLD-RBR | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| CLD-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

| | | | |
|---|---|---|---|
| CLD-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

***Tabla 5.6.***Tipos de Conectividad Cliente-ISPs [CLIENTE D]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CLE-RG1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| CLE-RG2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| CLE-RS1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |
| CLE-RS2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |

Tabla 5.7. Tipos de Conectividad Cliente-ISPs [CLIENTE D]

**Tablas *Community* publicadas por ambos ISPs:**

| Tipo QoS | Tipo Dirección | Ruta de respaldo | Etiqueta | Valor Community | Local Preference | Weight |
|---|---|---|---|---|---|---|
| Normal | PA | Si | 1 | no-export 100:1 | 50 | 0 |
| Normal | PA | | 2 | no-export 100:2 | 120 | |
| Normal | PI | Si | 3 | 100:3 | 50 | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Normal | PI | | 4 | 100:4 | 120 | |
| Gold | PA | Si | 5 | no-export 100:5 | 50 | 0 |
| Gold | PA | | 6 | no-export 100:6 | 120 | |
| Gold | PI | Si | 7 | 100:7 | 50 | 0 |

Tabla 5.8. Tipos de Conectividad Cliente-IPS [Communities ISP X]

| Tipo QoS | Tipo Dirección | Ruta de respaldo | Etiqueta | Valor Community | Local Preference | Weight |
|---|---|---|---|---|---|---|
| Normal | PA | Si | 1 | no-export 200:1 | 50 | 0 |
| Normal | PA | | 2 | no-export 200:2 | 120 | |
| Normal | PI | Si | 3 | 200:3 | 50 | 0 |
| Normal | PI | | 4 | 200:4 | 120 | |
| Gold | PA | Si | 5 | no-export 200:5 | 50 | 0 |
| Gold | PA | | 6 | no-export 200:6 | 120 | |
| Gold | PI | Si | 7 | 200:7 | 50 | 0 |
| Gold | PI | | 8 | 200:8 | 120 | |

Tabla 5.9. Tipos de Conectividad Cliente-IPS [Communities ISP Y]

## 5.5. DESCRIPCIÓN DE LA ACTIVIDAD

### TAREA 1: Diseñar y documentar un esquema de direccionamiento

**Paso 1:** Diseñe un esquema de direccionamiento.

Utilice la topología mostrada previamente y diseñe el esquema de direccionamiento con base en los siguientes requisitos:

- El espacio de dirección para la red del cliente A es el bloque de direcciones PA asignado por el ISPX 11.1.0.0/17. Deberá asignar a cada router de sucursal (CLA-RS1, CLA-RS2y CLA-RS3) un espacio de dirección según estos requisitos. Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router.

  - CLA-RS1 necesita espacio para 16 000 hosts _____
  - CLA-RS2 necesita espacio para 8000 hosts _____
  - CLA-RS3 necesita espacio para 8000 hosts _____

- Divida el espacio de dirección para cada router de sucursal en tres subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLA-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLA-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLA-RS3 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

- Para las WAN en la red del cliente A, realice una conexión con una subred en la dirección 10.1.128.0/28. La conexión CLA-RS1 a CLA-RG utiliza la primera subred, la conexión CLA-RS2 a CLA-RG utiliza la segunda y la conexión CLA-RS3 a CLA-RG, la tercera. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLA-RS1 <> CLA-RG | 0 | | |
| CLA-RS2 <> CLA-RG | 1 | | |
| CLA-RS3 <> CLA-RG | 2 | | |

- El espacio de dirección para la red delcliente B es el bloque de direcciones PA 11.1.128.0/18asignado por el ISPX. Deberá asignar a cada router de sucursal (CLB-RS1, CLB-RS2 y CLB-RS3) un espacio de dirección según estos requisitos. Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router.

  - CLB-RS1 necesita espacio para 8000 hosts _____
  - CLB-RS2 necesita espacio para 4000 hosts _____
  - CLB-RS3 necesita espacio para 4000 hosts _____

- Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLB-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLB-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLB-RS3 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

- Para las WAN en la red del cliente B, realice una conexión con una subred en la dirección 10.2.128.0/27. La conexión CLB-RS1 a CLB-RBR utiliza la primera subred, la conexión CLB-RS2 a CLB-RBR utiliza la segunda, la conexión CLB-RS3 a CLB-RBR utiliza la tercera, la conexión CLB-RG1 a CLB-RBR, la cuarta y la conexión CLB-RG2 a CLB-RBR utiliza quinta. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLB-RS1 <> CLB-RBR | 0 | | |
| CLB-RS2 <> CLB-RBR | 1 | | |
| CLB-RS3 <> CLB-RBR | 2 | | |
| CLB-RG1 <> CLB-RBR | 3 | | |
| CLB-RG2 <> CLB-RBR | 4 | | |

- El espacio de dirección para la red del cliente C es el bloque de direcciones PA asignado por el ISPX 11.1.192.0/19. Deberá asignar a cada router de sucursal (CLC-RS1, CLC-RS2) un espacio de dirección según estos requisitos. Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router.

  - CLC-RS1 necesita espacio para 4000 hosts _____
  - CLC-RS2 necesita espacio para 2000 hosts _____

- Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla.

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLC-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLC-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

- Para las WAN en la red del cliente C, realice una conexión con una subred en la dirección 10.3.128.0/28. La conexión CLC-RS1 a CLC-RG utiliza la primera subred, la conexión CLC-RS2 a CLC-RG, la segunday la conexión CLC-RS1 a CLC-RS2 utiliza la tercera subred. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLC-RS1 <> CLC-RG | 0 | | |
| CLC-RS2 <> CLC-RG | 1 | | |
| CLC-RS1 <> CLC-RS2 | 2 | | |

- El espacio de dirección para la red del cliente D es el bloque de direcciones PA asignado por el ISPX 11.1.224.0/20. Deberá asignar a cada router de sucursal (CLD-RS1 y CLD-RS2) un espacio de dirección según estos requisitos. Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router.

  - CLD-RS1 necesita espacio para 2000 hosts _____
  - CLD-RS2 necesita espacio para 1000 hosts _____

- Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLD-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLD-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

- Para las WAN en la red del cliente D, realice una conexión con una subred en la dirección 10.4.128.0/27. La conexión CLD-RS1 a CLD-RBR utiliza la primera subred, la conexión CLD-RS2 a CLD-RBR utiliza la segunda, la conexión CLD-RG1 a CLD-RBR la tercera y la conexión CLD-RG2 a CLD-RBR utiliza cuarta. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLD-RS1 <> CLD-RBR | 0 | | |
| CLD-RS2 <> CLD-RBR | 1 | | |
| CLD-RG1 <> CLD-RBR | 2 | | |
| CLD-RG2 <> CLD-RBR | 3 | | |

- El espacio de dirección para la red del cliente E es el bloque de direcciones PI 12.0.0.0/16. Deberá asignar a cada router de sucursal (CLE-RS1, CLE-RS2) un espacio de dirección según estos requisitos. Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router.

  - CLE-RS1 necesita espacio para 32000 hosts _____
  - CLE-RS2 necesita espacio para 16000 hosts _____

- Divida el espacio de dirección para cada router de sucursal en tres subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLE-S1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CLE-S2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

- Para las WAN en la red del cliente E, realice una conexión con una subred en la dirección 10.5.128.0/27. La conexión CLE-RG1 <> CLE-RG2 utiliza la primera subred, la conexión CLE-RG1<> CLE-S1utiliza la segunda, la conexión CLE-RG1 <> CLE-RS2 utiliza la tercera, la conexión CLE-RG2 <> CLE-RS1 la cuarta, y por últimola conexión CLE-RG2 <> CLE-RS2 utiliza quinta.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLE-RG1 <> CLE-RG2 | 0 | | |
| CLE-RG1 <> CLE-RS1 | 1 | | |
| CLE-RG1 <> CLE-RS2 | 2 | | |
| CLE-RG2 <> CLE-RS1 | 3 | | |
| CLE-RG2 <> CLE-RS2 | 4 | | |

- Para las WAN en la red del ISP X, realice una conexión con una subred en la dirección 172.16.0.0/28. La conexión ISPX-R1 a ISPX-R2 utiliza la primera subred, la conexión ISPX-R1 a ISPX-R3 utiliza la segunda, la conexión ISPX-R2 a ISPX-R3 utiliza la tercera. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| ISPX-R1 <>ISPX-R2 | 0 | | |
| ISPX-R1 <>ISPX-R3 | 1 | | |
| ISPX-R2 <>ISPX-R3 | 2 | | |

- Para las WAN en la red del ISP Y, realice una conexión con una subred en la dirección 172.17.0.0/28. La conexión ISPY-R1 a ISPY-R2 utiliza la primera subred, la conexión ISPY-R1 a ISPY-R3 utiliza la segunda, la conexión ISPY-R2 a ISPY-R3 utiliza la tercera. Registre las subredes.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| ISPY-R1 <> ISPY-R2 | 0 | | |
| ISPY-R1 <> ISPY-R3 | 1 | | |
| ISPY-R2 <> ISPY-R3 | 2 | | |

- Para las WAN que conectan los clientes A, B, C, D y E a los proveedores de servicio, utilice la subred en la dirección 192.168.0.0/26.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CLA-RG <> ISPX-R1 | 0 | | |
| CLB-G1 <> ISPX-R3 | 1 | | |
| CLB-G2 <> ISPX-R2 | 2 | | |
| CLC-RG <> ISPX-R1 | 3 | | |
| CLC-RG <> ISPX-R1 | 4 | | |
| CLD-G1 <> ISPX-R3 | 5 | | |
| CLD-G2 <> ISPX-R2 | 6 | | |
| CLE-G1 <> ISPX-R1 | 7 | | |
| CLE-G2 <> ISPY-R1 | 8 | | |
| ISPX-R2 <> ISPY-R2 | 9 | | |

**Paso 2:** Documente el esquema de direccionamiento.

- Documente las direcciones IP y máscaras de subred. Para los routers de sucursal asigne la primera dirección IP a la interfaz del router.
- En los enlaces WAN entre el cliente A, B, C, D y E y los ISPs utilice la primera dirección IP para los routers de borde de ambos ISPs.

## TAREA 2: Aplicar una configuración básica

**Paso 1:** Conecte una red que sea similar a la del diagrama de topología.

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en el gráfico.

**Paso 2:** Configuración básica de los enrutadores.

Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautasgenerales (utilice como contraseña la palabra *"nyquist"*):

1. Configure el nombre de host del router.
2. Configure una contraseña de modo EXEC privilegiado.
3. Configure un mensaje del día.
4. Configure una contraseña para las conexiones de la consola.
5. Configure una contraseña para las conexiones de VTY.

## TAREA 3: Configurar el enrutamiento dinámico

**Paso 1:** Configurar el enrutamiento OSPF en ambos ISPs.

Configure el enrutamiento OSPF (proceso ID 1) en cada router de cada ISP.

**Paso 2:** Configurar el enrutamiento RIPv2 en los clientes A Y B.

- Configure todos los routers en la red de ambos clientes con RIPv2 como protocolo de enrutamiento dinámico. Deshabilite la sumarización automática.
- Deshabilite las actualizaciones RIP en las interfaces apropiadas.

**Paso 3:** Configurar el enrutamiento EIGRP en los cliente C, D y E.

Configure todos los dispositivos con un enrutamiento EIGRP en la red de los clientes C, D y E. En la configuración, asegúrese de:

- Desactivar la sumarización automática.
- Detener las actualizaciones de enrutamiento en las interfaces que no estén conectadas a los vecinos de EIGRP.

## TAREA 4: Establezca las configuraciones pertinentes en ambos ISPs

**Paso 1:** Establecer mallas completas de sesiones IBGP en cada ISP.

- Utilice el comando neighbor <ipaddress> remote-as <as-number> en el modo de configuración del router para crear mallas completas de sesiones IBGP al interior de ambos ISPs.
- Asegúrese de utilizar interfaces Loopback para establecer las sesiones IBGP mediante el comando de configuración router neighbor <ip-address> update-source <interface>.

Establezca una malla completa de sesiones IBGP en el ISP X.

Establezca sesiones IBGP entre todos los routers de borde del ISP X.

Establezca una malla completa de sesiones IBGP en el ISP Y.

Establezca sesiones IBGP entre todos los routers de borde del ISP Y.
**Paso 2:** Establezca los filtros adecuados.

- Establezca los filtros adecuados en ambos ISPs que cumplan con los requerimientos que reflejan las tablas community publicadas.
- Asegúrese que el ISP no anuncie las rutas PA del cliente hacia Internet. Establezca esta configuración con la función community apropiada consignada en las tablas publicadas por ambos ISPs.

- Para cada cliente establezca un filtro para las actualizaciones entrantes con el objetivo de verificar que cada cliente anuncie solo el bloque de direcciones asignado.
- Establezca otro filtro para las actualizaciones entrantes para cada cliente que permita verificar que cada uno de los clientes anuncia solo las rutas de origen en su AS. Asegúrese de que cada filtro permita la configuración de la función AS-path prepending en cada cliente.

## TAREA 5: Establezca conectividad entre el cliente A y el ISP X usando enrutamiento estático

Como muestra la topología, el cliente A se conecta físicamente al ISP X a través de un único enlace. En esta configuración el router de borde del cliente A se conecta a través de un enlace de 2 Mbps a uno de los routers de borde del ISP X.

En este tipo de conexión cualquier tipo de falla en el enlace, fallas en uno de los routers de borde involucrados en la conexión o fallas al interior de la red del ISP causara una interrupción completa del servicio.

**Paso 1:** Configure la conectividad a nivel del cliente.

- Cree en el router de borde una ruta estática por defecto que apunte a la interface serial adecuada.
- Redistribuya la ruta estática por defecto en el proceso de enrutamiento RIPv2 del router de borde mediante el comando de configuración de router default-information originate.

**Paso 2:** Configure la conectividad a nivel del ISP X.

Antes de establecer la configuración responda:

¿Qué es un bloque de direcciones PA?

_____
_____
_____.

¿Qué tipo de clientes utilizan direcciones PA?, ¿Por qué?

_____
_____
_____
_____.

¿Por qué el ISP no anuncia las direcciones PA de sus clientes como rutas explícitas al resto de internet?

_____
_____
_____
_____.

- En el router de borde del ISP utilizado para establecer la conexión con el cliente configure una ruta estática que apunte a la red del cliente utilizando la interface serial adecuada. No olvide utilizar la etiqueta apropiada.
- Redistribuya la ruta estática en el proceso de enrutamiento BGP.

**Nota:** asegúrese que el ISP no anuncie las rutas del cliente al resto de Internet. Utilice la tabla publicada por el ISPX para establecer las configuraciones adecuadas con el fin de lograr los requerimientos planteados.

Existe un valor community predefinido que puede ser utilizado para lograr este objetivo, ¿cuál es? _____.

## TAREA 6: Establezca conectividad entre el cliente B y el ISP X usando enrutamiento estático

Como muestra la topología, el cliente B se conecta físicamente al ISP X a través de dos enlaces independientes. En esta configuración el router de borde principal del cliente se conecta a través del enlace principal de 2 Mbps a uno de los routers de borde del ISP X, mientras que el router de borde de respaldo se conecta a otro router de borde diferente del ISP a través de un enlace de respaldo de 64 kbps. Si uno de los dos enlaces o los routers de borde involucrados en dicha conexión fallan, la otra conexión aún está disponible.

En este tipo de conexión cualquier tipo de falla al interior de la red del ISP causara una interrupción completa del servicio.

Antes de establecer las configuraciones pertinentes responda:

¿Bajo qué circunstancias es posible utilizar enrutamiento estático para establecer la conexión entre un cliente y un ISP cuando existen múltiples conexiones independientes entre ellos?

_____
_____
_____
_____.

**Configure la conectividad a nivel del cliente.**

**Paso 1:** Configure el router de borde principal.

- Cree una ruta estática por defecto que apunte a la interface serial adecuada.
- Redistribuya la ruta estática por defecto en el proceso de enrutamiento RIPv2 del router de borde mediante el comando de configuración de router default-informationoriginate.

**Paso 2:** Configure el router de borde de respaldo.

- Cree una ruta estática por defecto flotante que apunte a la interface serial adecuada.
- Redistribuya la ruta estática flotante en el proceso de enrutamiento RIPv2 del router de borde mediante el comando de configuración de router default-informationoriginate.

**Nota:** Asegúrese que la ruta flotante tenga una AD mayor a la AD del IGP que ejecuta el cliente.

¿Qué es una ruta estática flotante?

_____
_____
_____.

¿Por qué razón es necesario establecer una ruta estática flotante en el router de respaldo con una AD mayor a la AD del IGP que se ejecuta al interior de la red del cliente?
_____
_____
_____
_____
_____.

Describa de forma precisa el proceso de redistribución y selección de las rutas estáticas al interior de la red del cliente en circunstancias normales (mientras ambos enlaces están up).
_____
_____
_____
_____
_____.

Describa de forma precisa el proceso de redistribución y selección de las rutas estáticas al interior de la red de cliente si el enlace principal falla.
_____
_____
_____
_____
_____.

Describa de forma precisa el proceso de redistribución y selección de las rutas estáticas al interior de la red de cliente si el enlace principal se restablece.

_____
_____
_____
_____.

**Configure la conectividad a nivel del ISP X.**

**Paso 1:** Configure el router de borde utilizado para la conexión principal.

- En el router de borde del ISP utilizado para establecer la conexión principal con el cliente configure una ruta estática que apunte a la red del cliente utilizando la interface serial adecuada.
- Redistribuya la ruta estática en el proceso de enrutamiento BGP.

**Nota:** asegúrese que el ISP no anuncie las rutas del cliente al resto de Internet.

**Paso 2:** Configure el router de borde utilizado para la conexión de respaldo.

- En el router de borde del ISP utilizado para establecer la conexión de respaldo con el cliente configure una ruta estática flotante que apunte a la red del cliente utilizando la interface serial adecuada.
- Redistribuya la ruta estática en el proceso de enrutamiento BGP.

**Nota:** Asegúrese que la ruta flotante tenga una AD mayor a la AD de BGP.

¿De acuerdo al proceso de selección de ruta BGP, que posibles problemas pueden ocasionar la redistribución de rutas estáticas flotantes en un entorno BGP?

_____
_____
_____
_____
_____.

Simule un fallo en el enlace principal, después de unos segundos restablezca la conexión a través de dicho enlace. Utilice el comando **show ip bgp** acompañado de la ruta del cliente en el router de borde utilizado para la conexión de respaldo.

Note que este router tiene dos rutas alternativas para esta red de destino, note además que a pesar que la conexión a través del enlace principal ya está restablecida este router de borde selecciona la ruta que ha redistribuido en BGP usando la ruta estática flotante.

¿A qué se debe este comportamiento no deseado?

_____
_____
_____
_____
_____.

¿Qué configuraciones adicionales debe establecer en este router para que seleccione nuevamente la ruta principal una vez esta se haya restablecido?

_____
_____
_____
_____.

**Paso 3:** Establezca las configuraciones adicionales.
Establezca las configuraciones pertinentes para que este router seleccione la ruta estática principal una vez la conexión principal se encuentre de nuevo activa. Utilice la tabla del ISPX para cumplir con este requerimiento.

## TAREA 7: Establezca un escenario *Load Sharing* en cliente C mediante la función EBGP *multihop*

En este escenario las redes del cliente y el ISP están conectados a través de dos enlaces paralelos entre un único router en la AS del cliente y un único router en la red del ISP. En este tipo de conexión si uno de los dos enlaces falla, la otra conexión aún está disponible.

Si se presentan fallos los routers de borde involucrados en dicha conexión o cualquier tipo de falla al interior de la red del ISP se interrumpirá completamente el servicio.

Utilizar interfaces *Loopback* en cada router para establecer la conexión permite que se establezca una única sesión EBGP entre ambos routers independientemente del número de enlaces que los conectan.

Debido a que la sesión no se establece a través de interfaces directamente conectadas es necesario llevar cabo un búsqueda recursiva para resolver las direcciones *Loopback* de siguiente salto implementando ya sea un esquema de enrutamiento estático o dinámico y configurar además la función **EBGP multihop** ya que de otro modo la sesión EBGP no abandonará el estado IDLE.

Como se mencionó antes esta implementación se puede llevar a cabo ya sea mediante enrutamiento dinámico o enrutamiento estático.

**NOTA:** En ambos casos asegúrese de utilizar la función **EBGP multihop** para garantizar que la sesión sea completamente establecida.

¿Por qué es necesario configurar la función **EBGP multihop** en ambos routers de borde para establecer la sesión EBGP a través de sus interfaces *Loopback*?

_____
_____
_____.

**Garantice búsqueda recursiva y la conexión mediante de rutas estáticas.**

**Paso 1:** Configure la conectividad a nivel del cliente.

- Configure la interfaz Loopback 0 del cliente con la dirección 1.1.1.1
- Asegúrese que las interfaces seriales involucradas en la conexión estén configuradas correctamente.
- Establezca la sesión EBGP con el router del ISP y asegúrese de que la interfaz de origen para la conexión sea la interfaz Loopback ya configurada.
- Configure dos rutas estáticas para la interfaz Loopback del router vecino que apunten a la interfaz serial respectiva del vecino.
- Cree una ruta estática que cubra todo el espacio de direcciones PA del cliente y apunte al núcleo de la red del cliente.
- Anuncie el espacio de direccionamiento PA a través del comando network.

**Paso 2:** Configure la conectividad a nivel del ISP.

- Configure la interfaz Loopback 0 del ISP con la dirección 2.2.2.2
- Asegúrese que las interfaces seriales involucradas en la conexión estén configuradas correctamente.
- Establezca la sesión EBGP con el router del cliente y asegúrese de que la interfaz de origen para la conexión sea la interfaz Loopback ya configurada.
- Configure dos rutas estáticas para la interfaz Loopback del router vecino que apunten a la interfaz serial respectiva.
- Anuncie una ruta por defecto al cliente a través de BGP en el router de borde del ISP mediante el comando de configuración de routerneighborip-addressdefault-originate. Asegúrese que el ISP solo anuncia la ruta por defecto a dicho cliente mediante la configuración de un filtro de salida.
- Asegúrese que el ISP no anuncie las rutas PA del cliente hacia Internet. Cerciórese que la configuración sea correcta con la ayuda de las tablas publicadas por ambos ISPs.

**NOTA 1**: Asegúrese de utilizar la función **EBGP multihop** para garantizar que la sesión sea completamente establecida.

**NOTA 2:**Asegúrese de redistribuir esta ruta por estática defecto en el router del cliente.

**Garantice la búsqueda recursiva y la conexión a través del IGP.**

**Paso 1:** Configure la conectividad a nivel del cliente.

- Configure la interfaz Loopback 0 del cliente con la dirección 1.1.1.1
- Asegúrese que las interfaces seriales involucradas en la conexión estén configuradas correctamente.
- Establezca la sesión EBGP con el router del ISP y asegúrese de que la interfaz de origen para la conexión sea la interfazLoopback ya configurada.
- Debe garantizar que el IGP que se ejecuta en la red del cliente tenga información de enrutamiento acerca de las interfaces que conectan ambos routers de borde.
- Anuncie el espacio de direccionamiento PA a través del comando network.

**Paso 2:** Configure la conectividad a nivel del ISP.

- Configure la interfaz Loopback 0 del ISP con la dirección 2.2.2.2
- Asegúrese que las interfaces seriales involucradas en la conexión estén configuradas correctamente.
- Establezca la sesión EBGP con el router del cliente y asegúrese de que la interfaz de origen para la conexión sea la interfaz Loopback ya configurada.
- Debe garantizar que el IGP que se ejecuta en la red del ISP tenga información de enrutamiento acerca de las interfaces que conectan ambos routers de borde.
- Anuncie una ruta por defecto al cliente a través de BGP en el router del borde del ISP mediante el comando de configuración de routerneighborip-addressdefault-originate. Asegúrese que el ISP solo anuncia la ruta por defecto a dicho cliente mediante la configuración de un filtro de salida.

Describa el proceso de búsqueda recursiva a nivel general para la dirección *Loopback*de siguiente salto, y la instalación subsecuente de ruta en la tabla de enrutamiento cuando se recibe una ruta EBGP en un escenario como este.

_____
_____
_____
_____
_____.

¿Al utilizar interfaces *Loopback* para establecer una sesión EBGP es posible balancear carga independientemente del número de conexiones existentes entre ambos routers de borde? ¿Por qué?

_____
_____
_____
_____.

## TAREA 8: Establezca conectividad entre el cliente D y el ISP X a través de BGP

Este escenario es similar al escenario B, ya que la conexión entre el cliente y el ISP se establece a través de múltiples enlaces independientes y se establece una configuración primary/backup. La única diferencia es que el método de intercambio de información de enrutamiento cambia.

En este escenario los routers de borde del cliente anuncian su espacio de direccionamiento PA al ISP a través de BGP. La red del cliente no contará con información de enrutamiento completa de internet; en su lugar los routers de borde del ISP anunciaran solo una ruta estática por defecto. Los routers de borde del ISP deben establecer filtros de entrada para depurar las actualizaciones del cliente.

¿Bajo qué circunstancias es posible utilizar BGP para establecer la conexión entre un cliente y un ISP cuando existen múltiplesconexiones independientes entre ellos?

_____
_____
_____
_____.

**Configure la conectividad a nivel del cliente.**

Antes de establecer la configuración responda:

¿Es necesario establecer una malla completa de sesiones IBGP al interior de la red del cliente? ¿Por qué?

_____
_____
_____.

- Establezca una sesión IBGP entre los routers de borde del cliente.
- Establezca sesiones EBGP con los routers de borde del ISP.
- Anuncie el espacio de direccionamiento PA a través del comando network.

Cree una ruta estática que cubra todo el espacio de direcciones PA del cliente y apunte al núcleo de la red del cliente.
¿Cuál es el objetivo de crear una ruta estática que cubra todo el espacio de direcciones PA del cliente?

_____
_____
_____
_____.

¿A qué hace referencia el término "núcleo de la red"?
_____
_____.

¿Por qué en necesario que dicha ruta estática apunte al núcleo de la red del cliente? _____
_____
_____
_____
___.

**Nota:** Tenga en cuenta que el cliente obtendrá acceso a internet a través de la ruta estática por defecto que el ISP anunciará. Asegúrese de redistribuir esta ruta en el Protocolo de Gateway Interior que se ejecuta al interior de la red del cliente de modo que los demás routers de la red tengan conocimiento acerca del punto de salida del AS.

**Configure la conectividad a nivel del ISP**

- Establezca sesiones EBGP con los routers de borde del cliente.
- Anuncie una ruta por defecto al cliente a través de BGP en los routers de borde del ISP mediante el comando de configuración de routerneighborip-addressdefault-originate. Asegúrese que el ISP solo anuncia la ruta por defecto a dicho cliente mediante la configuración de un filtro de salida.
- Para cada cliente cree un filtro para las actualizaciones entrantes con el objetivo de verificar que cada cliente anuncie solo el bloque de direcciones asignado.
- Asegúrese deestablecer un filtro para las actualizaciones entrantes para cada cliente que permita verificar que cada uno de los clientes anuncia solo las rutas de origen en su AS.Asegúrese de que cada filtro permita la configuración de la función AS-pathprepending en cada cliente.
- Asegúrese que el ISP no anuncie las rutas PA del cliente hacia Internet. Establezca esta configuración con la ayuda de las tablas publicadas por ambos ISPs.

**Elimine los números AS privados**

Para evitar que el número AS privado del cliente sea propagado por los routers de borde del ISP al resto de internet elimínelo mediante el comando de configuración de router **neighbor** {*ip-address--peer-group-name*} **remove-private-as** en los routers de egreso adecuados.

¿Por qué es necesario que los routers de egreso del ISP eliminen los números AS privados que identifican a sus clientes, con el objetivo de no propagar dichos números AS al resto de Internet?
_____
_____
_____
_____.

**Establecer una configuración primary/backup.**
Utilice los atributos de ruta BGP para establecer una configuración en la que el enlace de 2 Mbps que une el cliente al ISP actué como enlace principal y el enlace restante de 64 Kbps se utilice solo para propósitos de respaldo. Asegúrese que la información de enrutamiento a nivel del cliente fluya de forma simétrica.

## TAREA 9: Establezca conectividad entre el cliente E y ambos ISP mediante BGP implementando una configuración primary/backup

Como muestra la topología, el cliente E tiene dos enlaces independientes que lo conectan a internet a través de dos ISPs diferentes. En esta configuración el router de borde principal del cliente se conecta a través del enlace principal de 2 Mbps a uno de los routers de borde del ISPX, mientras que el router de borde de respaldo se conecta a uno de los routers de borde del ISPY a través de un enlace de respaldo de 64 Kbps.

Esta forma de conexión ofrece el mayor nivel de flexibilidad para cualquier tipo de falla.

Utilice los atributos de ruta BGP para establecer una configuración en la que el enlace de 2 Mbps que une el cliente al ISPX actué como enlace principal y el enlace restante de 64 Kbps que lo une al ISPY se utilice solo para propósitos de respaldo. Asegúrese que tanto la información de enrutamiento a nivel del cliente fluya de forma simétrica.

Antes de establecer la configuración analice y responda:

¿Por qué el uso de rutas estáticas no funciona adecuadamente en este tipo de escenario?
_____
_____
_____.

¿Por qué razón los enlaces que conectan la red del cliente con ambos ISPs deben finalizar en routers de borde independientes en el lado del cliente?
_____
_____
_____.

**Paso 1:** establezca las configuraciones previas.

- Establezca una maya complete de sesiones IBGP en la red del cliente.
- Asegúrese de que el cliente no actúe como un AS de tránsito para ambos ISPs.

**Paso 2:** seleccione el enlace correcto para el fluyo de salida.

Establezca el o los valores correctos *local preference***.**

**Paso 3:** seleccione el enlace correcto para el fluyo de entrada.

Para cumplir con este objetivo puede utilizar la función *AS-pathprepending*o los valores *community* apropiados de acuerdo a las tablas publicadas por ambos ISPs.

## TAREA 10: En el ISPX anuncie el bloque de direcciones mayor

Anuncie en los routers de borde adecuados el bloque de direcciones mayor al que pertenecen los bloques de direcciones PA asignados a cada uno de los clientes pertinentes.

## TAREA 11: Examinar la conectividad

Asegúrese que haya conectividad total en todo el escenario de red de la topología. Si no existe conectividad completa, corrija los posibles errores hasta que haya conectividad completa.

## TAREA 12: Eliminar la configuración *primary/backup* del cliente B y establezca un escenario *Load Sharing*

**Paso 1:** Elimine la configuración *primary/backup* del cliente B.

Elimine las configuraciones pertinentes que permiten al router seleccionar la ruta estática principal una vez la conexión principal se encuentre de nuevo activa.

**Paso 2:** Establezca la configuración *Load Sharing* para el tráfico de salida.

El balanceo de carga para el tráfico de salida se logra estableciendo rutas estáticas por defecto estándar en ambos routers de borde del cliente.

**Paso 3:** Establezca la configuración *Load Sharing* para el tráfico entrante.

Para establecer una configuración de balanceo de carga a través de rutas estáticas es necesario dividir el bloque de direcciones del cliente y anunciar dichas fracciones a los demás routers del ISP, de este modo el tráfico con destino a una de los sub-bloques del bloque de direcciones real será enrutado a través de uno de los enlaces y el trafico dirigido al otro sub-bloque fluirá a través del otro enlace.

- Asegúrese que el router de borde principal anuncie la mitad del bloque de direcciones principal a los demás routers al interior de la red del ISP y el router restante anuncie la otra mitad.
- Asegúrese además que ambos routers de borde anuncien el bloque de direcciones completo, de este modo, en caso de presentarse una falla en uno de los enlaces o en

uno de los routers de borde para un de las conexiones, la información con destino a la otra mitad del bloque de direcciones no anunciado por el router fallido fluirá a través del enlace restante.
- Establezca las communities apropiadas de modo que las direcciones PA del cliente no sean anunciadas a internet de acuerdo a las tablas publicadas.

## TAREA 13: Eliminar la configuración *primary/backup* del cliente D y establezca un escenario Load Sharing mediante la función *EBGP multipath*

De forma predeterminada el proceso de enrutamiento BGP selecciona sola una ruta a un destino en particular y la instala en la tabla de enrutamiento. Si el cliente anuncia rutas equivalentes a través de ambos enlaces mediante BGP los routers al interior del ISP usaran la conexión más próxima de acuerdo a la información proporcionada por el IGP. Una forma de lograr un balanceo de carga para el tráfico entrante es utilizar la opción ***EBGP multipath*** en los routers de borde del ISP de modo que el proceso de selección de ruta BGP seleccionará más de una ruta a una red específica y las instalará en la tabla de enrutamiento si dichas rutas son rutas equivalentes.

¿Qué son rutas equivalentes?

_____
_____.

**Paso 1:** Establezca la configuración *Load Sharing* para el tráfico de salida.

Asegúrese que los routers de borde del cliente envíen el tráfico hacia el ISP a través de ambos enlaces de forma equitativa.

**Paso 2:** Establezca la configuración *Load Sharing* para el tráfico de retorno.

Configure la función *BGP multipath* mediante el comando de configuración de router**máximum-paths***number* en los routers de borde adecuados.

## TAREA 14: Eliminar la configuración *primary/backup* del cliente E y establezca un escenario *Load Sharing*

**Paso 1:** Elimine la configuración *primary/backup* del cliente E.

Elimine las configuraciones pertinentes que permiten al router seleccionar el enlace que conecta el cliente con el ISPX como el enlace y el enlace que conecta el cliente con el ISP Y como el enlace de respaldo.

**Paso 2:** Establezca la configuración *Load Sharing* para el tráfico entrante.

Para establecer una configuración de balanceo de carga en este tipo de configuración mediante BGP es necesario dividir el bloque de direcciones del cliente y anunciar dichas subbloques asegurándose de enviar un bloque a uno de los ISPs y el bloque restante al ISP restante, de este modo el tráfico con destino a una de los subbloques del bloque de direcciones real será enrutado a través de uno de los enlaces y el trafico dirigido al otro subbloque fluirá a través del otro enlace.Debe tenerse en cuenta que ambos routers de borde deben anunciar el bloque de direcciones completo, de este modo, en caso de presentarse una falla en uno de los enlaces o en uno de los routers de borde para un de las conexiones, la información con destino a la otra mitad del bloque de direcciones no anunciado por el router fallido fluirá a través del enlace restante.

- Asegúrese que el uno de los routers de borde anuncie la mitad del bloque de direcciones principal a los demás routers al interior de la red del ISP y el router restante anuncie la otra mitad.
- Asegúrese además que ambos routers de borde anuncien el bloque de direcciones completo.

## TAREA 15: Examine la conectividad

Asegúrese que haya conectividad total en todo el escenario de red de la topología. Si no existe conectividad completa, corrija los posibles errores hasta que haya conectividad completa.

# CAPÍTULO SEIS

# Índice lab**oratorio N° 6**



# Índice de Figuras



# Índice de Tablas

# 6. LABORATORIO N° 6 - ESCALANDO A REDES DE PROVEEDORES DE SERVICIO

## 6.1. INTRODUCCIÓN

La red típica de un proveedor de servicios consiste en un núcleo de red que conecta varios dispositivos de borde, los cuales pueden estar conectados a clientes o a otros proveedores de servicio. Estos dispositivos de los proveedores de servicio que conectan enlaces de acceso, están físicamente localizados en grupos, lo cuales son llamados **Puntos de Presencia (PoP)**. Por lo general, los PoPs son grupos de routers en los cuales terminan los enlaces de acceso. Los routers de borde que conectan a otros proveedores de servicio pueden en este sentido ser considerados como un PoP.[14]

Los routers de un PoP se conectan al núcleo de la red mediante una capa de routers de concentración. El núcleo de la red renvía paquetes entre PoPs, varios puntos de acceso de clientes, o puntos de conexión con otros proveedores de servicio.[15]

La red de un proveedor de servicio común ejecuta EBGP para intercambiar información de enrutamiento con diferentes proveedores de servicio, y EBGP o enrutamiento estático con sus clientes. Siendo necesario que los routers internos ejecuten BGP y sean actualizados con información de enrutamiento consistente, para poder manejar todas las rutas externas, y enrutar información a través de la red del proveedor de servicio.[16]

14 Cisco System Learning.Configuring BGP on Cisco Routers.Version 3.2. Volumen 2. Estados Unidos. 2005. p. 248

15 Ibíd., p.248.

16 Ibíd., p. 251.

En el enfoque tradicional, asegurar información de enrutamiento consistente se logra estableciendo una malla completa de sesiones IBGP entre todos los routers dentro de un AS. Sin embargo, una malla completa IBGP es ciertamente **no escalable**. Por lo tanto, se diseñaron varias herramientas para lograr los mismos resultados sin las restricciones de una malla completa.[17]

## 6.2. OBJETIVOS

- Planear la migración de la red BGP basada en una malla completa de sesiones IBGP, hacia una topología basada en la implementación de reflectores de ruta.
- Configurar y verificar la operación apropiada de reflectores de ruta para modificar las reglas de horizonte dividido de IBGP.
- Configurar y verificar la operación apropiada de reflectores de ruta jerárquicos.
- Configurar y verificar la operación apropiada de confederaciones para modificar el procesamiento del atributo AS-path de IBGP.

## 6.3. LABORATORIO NO. 6.1 - REFELECTORES DE RUTA

### 6.3.1 Diagrama de Topología

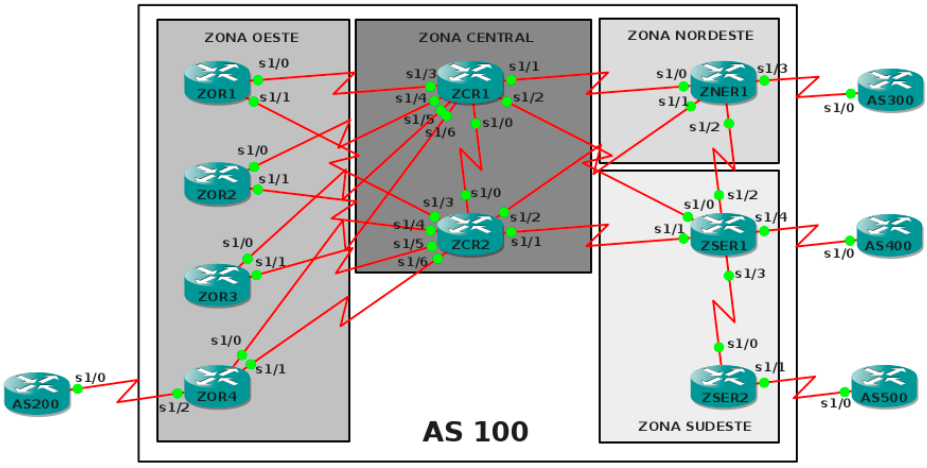


***Figura 6.1.*** Topología Reflectores de Ruta

17 Ibíd., p. 251.

## 6.3.2. TABLAS DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| ZCR1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Serial 1/5 | | |
| | Serial 1/6 | | |
| | Loopback0 | | |
| ZCR2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Serial 1/5 | | |
| | Serial 1/6 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| ZOR1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |
| ZOR2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |
| ZOR3 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |
| ZOR4 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| ZNER1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Loopback 0 | | |
| ZSER1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Loopback 0 | | |
| ZSER2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback 0 | | |

Tabla 6.1. Reflectores de Ruta

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| AS200 | Serial 1/0 | | |
| | Loopback0 | | |
| AS300 | Serial 1/0 | | |
| | Loopback0 | | |
| AS400 | Serial 1/0 | | |
| | Loopback0 | | |
| AS500 | Serial 1/0 | | |
| | Loopback0 | | |

Tabla 6.2. Reflectores de Ruta [AS Externos]

### 6.3.3. DESCRIPCIÓN DE LA ACTIVIDAD

### TAREA 1: División en subredes del espacio de direccionamiento

**Paso 1:** Examinar los requisitos de la red.

El direccionamiento para la red tiene los siguientes requisitos:

- Para el AS 100, el administrador de red de este AS, ha decidido utilizar los espacios de direcciones privadas 192.168.10.0/24 y 172.16.0.0/24, los cuales deben dividirse en subredes para proporcionar direcciones a las interfaces Loopback y a los enlaces seriales al interior del AS, respectivamente. Para facilitar la administración, el AS ha sido dividido en áreas según la distribución física de los routers al interior del mismo.

    - La zona oeste requerirá un espacio de direcciones, el cual se dividirá en 8 subredes, las cuales se asignarán a los enlaces seriales que conectan los routers de esta zona y los de la zona central. Cada router de esta zona requerirá una sola dirección IP para su propia interfaz Loopback.

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| ZCR1 <> ZOR1 | 0 | | |
| ZCR1 <>ZOR2 | 1 | | |
| ZCR1<>ZOR3 | 2 | | |
| ZCR1<>ZOR4 | 3 | | |
| ZCR2 <> ZOR1 | 4 | | |
| ZCR2 <>ZOR2 | 5 | | |
| ZCR2<>ZOR3 | 6 | | |
| ZCR2<>ZOR4 | 7 | | |

    - La zona estese ha divido en dos regiones, la región nordeste y la región sudeste; la región nordeste requerirá 3 subredes, las cuales se asignarán a los enlaces seriales que conectan los routers de esta región con los de la región sudeste, y los routers de la zona central; la región sudeste requerirá 3subredes, las cuales se asignarán a los enlaces que conectan a los routers de esta región entre sí y con los routers de la zona central. Cada router de esta zona requerirá una sola dirección IP para su propia interfaz Loopback.

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| ZCR1 <> ZNER1 | 0 | | |
| ZCR1 <>ZSER1 | 1 | | |
| ZCR2<>ZNER1 | 2 | | |
| ZCR2<>ZSER1 | 3 | | |
| ZNER1 <> ZSER1 | 4 | | |
| ZSER1 <>ZSER2 | 5 | | |

- La zona central, que en conjunto con los routers ZNER1 y ZSER1 forman el backbone de la red, requerirá una sola subred, la cual se asignará a los enlaces seriales que conectan a ambos routers. Cada router de esta zona requerirá una sola dirección IP para su propia interfaz Loopback.

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| ZNER1 <> ZNER2 | 0 | | |

- Para las conexiones externas entre los AS se ha asignado la red 209.128.0.0/28.

| Conexión | No. de Subred | Dirección Subred | Máscara Subred |
|---|---|---|---|
| ZCR1 <> ZNER1 | 0 | | |
| ZCR1 <>ZSER1 | 1 | | |
| ZCR2<>ZNER1 | 2 | | |
| ZCR2<>ZSER1 | 3 | | |
| ZNER1 <> ZSER1 | 4 | | |
| ZSER1 <>ZSER2 | 5 | | |

**Paso 2:** Documente el esquema de direccionamiento.

Documente las direcciones IP y máscaras de subred utilizando las tablas proporcionadas.

## TAREA 2: Preparación de la red

**Paso 1:** Conecte una red que sea similar a la del diagrama de topología.

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en el gráfico.

**Paso 2:** Configuración básica de los enrutadores.

Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautas generales (utilice como contraseña la palabra *"nyquist"*):

- Configure el nombre de host del router.
- Configure una contraseña de modo EXEC.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.
- Configure una contraseña para las conexiones de VTY.

## TAREA 3: Configurar y activar las interfaces

**Paso 1:** Configure las interfaces en los enrutadores con las direcciones IP de las tablas proporcionadas debajo del Diagrama de topología.

## TAREA 4: Configurar el protocolo de enrutamiento interno

**Paso 1:** Configurar el enrutamiento OSPF en cada uno de los routers del AS 100.

Configure todos los dispositivos con un enrutamiento OSPF en el AS 100. En la configuración, asegúrese de:

- Utilizar el Id de proceso 1 y el área 0 para las redes.
- Gracias a que se utiliza explícitamente un espacio de direccionamiento privado para los enlaces seriales internos y las interfaces Loopback, utilice el comando network junto con el espacio de direcciones de estas interfaces para establecer las interfaces que participaran en el enrutamiento OSPF.

**Nota:** Para este laboratorio, no es necesario redistribuir las redes de las interfaces directamente conectadas en las actualizaciones del enrutamiento OSPF.

## TAREA 5: Configurar el enrutamiento BGP en cada uno de los ASs

**Paso 1:** Configurar mallas completas de sesiones IBGP entre interfaces *Loopback* al interior del AS 100.

**Consulte y analice:**

¿Cuántas sesiones IBGP se debería establecer para configurar una malla completa al interior del AS 100?

¿Por qué la solución de implementar una malla completa sobre redes de proveedores de servicio no es una solución deseada a gran escala?

Establezca sesiones IBGP para el AS 100 a partir de las interfaces *Loopback* de los router.

Con el objetivo de que el IGP sea liberado de la responsabilidad de manejar información sobre los enlaces de acceso al AS y que no se vea afectado por un cambio de estado de dichos enlaces, se utiliza el comando **next-hop-self** sobre los PoPs de la red. El resultado de utilizar este comando permite que el atributo **next-hop** de las rutas hacia un determinado vecino sea establecido con la dirección *Loopback* del router de borde del proveedor de servicio y no con la dirección del enlace de acceso del cliente.

Configurar los PoPs de la red para que modifiquen el atributo **next-hop** de las rutas que son recibidas desde un AS externo, antes de ser publicadas a los demás routers internos. Utilice el comando:

**neighbor** *neighbor-ip-address* **next-hop-self**

**Paso 2:** Establecer sesiones EBGP.

Las sesiones EBGP entre ASs sólo se deben establecer entre los routers de borde entre interfaces directamente conectadas.

**Paso 3:** Habilitar la publicación de redes al interior de los ASs.

Desde los routers AS200, AS300, AS400 y AS500, publique la red que ha sido configurada sobre cada una de las interfaces *Loopback 0* de los routers.

**Paso 4:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS200 a la interfaz *Loopback 0* de los routers AS300, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS300 a la interfaz *Loopback 0* de los routers AS200, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS400 a la interfaz *Loopback 0* de los routers AS200, AS300 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS500 a la interfaz *Loopback 0* de los routers AS200, AS300 y AS400? SI ___ NO ___

¿Qué rutas BGP están presentes en la tabla de BGP del router ZCR1?

¿Qué rutas BGP están presentes en la tabla de BGP del router ZCR2?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS200?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS300?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS400?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS500?

## TAREA 6: Diseño y configuración de reflectores de ruta

El **reflector de ruta** actúa como punto de concentración para otros routers referidos como *clientes*. Los *clientes* se conectan como iguales con el reflector de ruta e intercambian información de enrutamiento con él. A su vez, el reflector de ruta pasa (o refleja) la información entre los clientes y a los otros iguales IBGP y EBGP.[18]

18 HALABI, Sam; MCPHERSON, Danny. Arquitectura de enrutamiento en Internet. Segunda Edición. Pearson Education. España. 2001. p. 245

**Paso 1:** Planeación y preparación de la red.

Los siguientes pasos de planificación y preparación son necesarios antes de migrar de una malla completa de sesiones IBGP a un diseño con reflector de ruta:

1. Identificar un grupo de routers periféricos que estén físicamente conectados al mismo conjunto de routers backbone. Se consideran los routers periféricos como clientes de reflector de ruta, y los routers backbone como reflectores de ruta. Se conforma un cluster con los routers anteriormente mencionados. Se debe asegurar que ningún router pertenezca a dos clusters diferentes, debido a que esto representaría una configuración errónea.

2. Crear un plan de enumeración que indique cuales números son asignados a los clusters en la red. En el plan se debe asegurar de que cada uno de los clusters dentro del AS este identificado de forma única. Los clusters no son vistos desde fuera del AS, así que el plan de enumeración no necesita coordinarse con ningún otro AS. Para facilitar la solución de problemas, se recomienda utilizar números menores que 256, debido a que los cluster-ID se muestran en formato de dirección IP.

Es importante tener presente que el uso de un diseño con reflectores de ruta hace una red bastante insensible a los errores de configuración. Para un desempeño óptimo, es necesaria una configuración óptima. Estos son algunos de los problemas que podrían presentarse si se desvía de las reglas de diseño de red de reflector de ruta:

- Si lo reflectores de ruta no están conectados a través de sesiones IBGP en una malla completa, algunos clusters no tendrían todas las rutas.
- Si un cliente tiene sesiones IBGP con algún reflector de ruta en un cluster pero no con todos, el cliente podría perder algunas rutas BGP.
- Si un cliente tiene sesiones IBGP con reflectores de ruta que pertenecen a diferentes clusters, la actualización BGP del cliente sería reenviada por él dentro de la malla completa con diferentes cluster-ID. Cuando la actualización entre a la malla, esta alcanzará a los otros reflectores de ruta, los cuales aceptarán la ruta, innecesariamente, como válida y la reenviarán dentro de sus clusters. Esta situación, a su vez, causará duplicación innecesaria de las actualizaciones de los clientes.
- Si un cliente tiene sesiones IBGP con otros clientes en el mismo cluster, estos clientes recibirán duplicaciones innecesarias de actualizaciones.

**Paso 2:** Migración de la red.

Como parte de la planificación y preparación necesaria para migrar de una malla completa de sesiones IBGP a un diseño con reflectores de ruta, se necesita realizar los siguientes cambios de configuración:

- Configurar el valor de cluster-ID apropiado en los reflectores de ruta.
- Configurar el reflector de ruta con información sobre las sesiones vecinas IBGP por las cuales está alcanzando a sus clientes.
- En los clientes, remover todas las sesiones IBGP a vecinos que no son reflectores de ruta en el cluster del cliente. Asegurarse que el vecino IBGP es removido en ambos extremos de la sesión IBGP

Para configurar el **cluster-ID**, si el cluster BGP tiene reflectores de ruta redundantes, utilice el comando en el modo de configuración de router:

**bgp cluster-id** *cluster-id*

Para configurar un router como un reflector de ruta BGP, y configurar un vecino específico como su cliente, se utiliza el comando:

**neighbor** *rrclient-ip-address* **route-reflector-client**

**Paso 3:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS200 a la interfaz *Loopback 0* de los routers AS300, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS300 a la interfaz *Loopback 0* de los routers AS200, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS400 a la interfaz *Loopback 0* de los routers AS200, AS300 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS500 a la interfaz *Loopback 0* de los routers AS200, AS300 y AS400? SI ___ NO ___

Utilice el siguiente comando para obtener información más detallada acerca de una red específica:

**show ip bgp** *network-ip-address* [*network-mask*]

Si las siguientes redes, están presentes en la tabla BGP del router ZCR1 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 20.0.0.0/24 _____
- 30.0.0.0/24 _____
- 40.0.0.0/24 _____
- 50.0.0.0/24 _____

Si las siguientes redes, están presentes en la tabla BGP del router ZOR4 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZNER1 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZSER1 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZSER2 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

# 6.4. LABORATORIO NO. 6.2 - REFELECTORES DE RUTA JERÁRQUICOS

## 6.4.1. DIAGRAMA DE TOPOLOGÍA

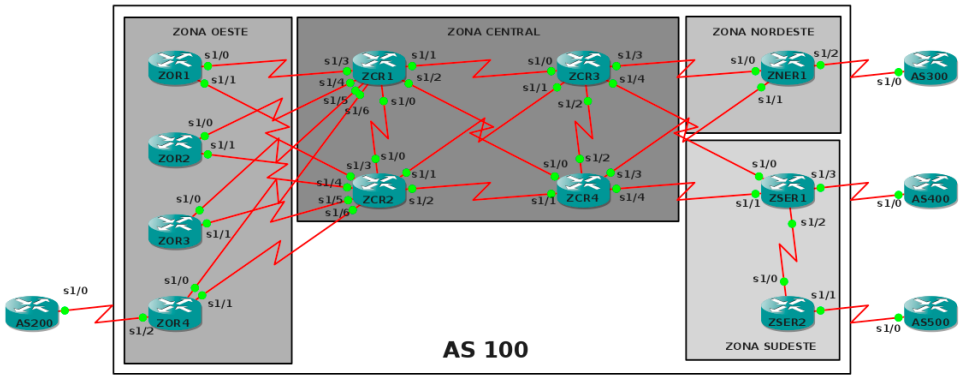


***Figura 6.2*** Topología Reflectores de Ruta Jerárquicos

## 6.4.2. TABLAS DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| ZCR1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Serial 1/5 | | |
| | Serial 1/6 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| ZCR2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Serial 1/5 | | |
| | Serial 1/6 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| ZCR3 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Loopback0 | | |
| ZCR4 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Loopback0 | | |
| ZOR1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| ZOR2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |
| ZOR3 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |
| ZOR4 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback0 | | |
| ZNER1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback 0 | | |
| ZSER1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Loopback 0 | | |
| ZSER2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback 0 | | |

Tabla 6.3. Reflectores de Ruta Jerárquicos [AS 100]

## 6.4.3. DESCRIPCIÓN DE LA ACTIVIDAD

## TAREA 1: Reestructuración y reconfiguración de la red

**Paso 1:** Reestructure la red para que sea similar a la del diagrama de la topología.

Con la red construida en el laboratorio de **reflectores de ruta** como base, reestructúrela como se indica en el diagrama de topología.

**Paso 2:** Reconfiguración de los dispositivos de la red.

Realice las configuraciones y modificaciones que considere pertinentes para que la red

existente tenga un comportamiento similar al que se muestra en la topología. Tenga en cuenta el direccionamiento necesario para las interfaces de los routers añadidos a la red, y configurar en ellos el protocolo de enrutamiento dinámico OSPF bajo las mismas especificaciones mencionadas en el laboratorio de **reflectores de ruta**.

Documente las direcciones a utilizarse en la tabla proporcionada debajo del diagrama de topología.

## TAREA 2: Configurar el enrutamiento BGP en cada uno de los ASs

**Paso 1:** Establecer sesiones IBGP.

**Consulte y analice:**

¿Cuántas sesiones IBGP se deberán establecer para configurar una malla completa al interior del AS 100?

¿Cuántas sesiones IBGP se deberán establecer para configurar un diseño con reflectores de ruta?

Construya un diseño con reflectores de ruta para el AS 100. Establezca sesiones IBGP a partir de las interfaces *Loopback* de los router, donde sea necesario. Recuerde implementar el comando **next-hop-self** sobre los routers de borde de la red.

**Paso 2:** Establecer sesiones EBGP.

Restablezca sesiones EBGP entre ASs donde considere que sea necesario, recuerde que sólo se deben establecer entre los routers de borde entre interfaces directamente conectadas.

**Paso 3:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

¿Es posible realizar un ping desde la interfaz *Loopback* 0 del router AS200 a la interfaz *Loopback* 0 de los routers AS300, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback* 0 del router AS300 a la interfaz *Loopback* 0 de los routers AS200, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback* 0 del router AS400 a la interfaz

*Loopback* 0 de los routers AS200, AS300 y AS500? SI ___ NO ___
¿Es posible realizar un ping desde la interfaz *Loopback* 0 del router AS500 a la interfaz *Loopback* 0 de los routers AS200, AS300 y AS400? SI ___ NO ___

Si las siguientes redes, están presentes en la tabla BGP del router ZCR1 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 20.0.0.0/24: _____
- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZCR3 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 20.0.0.0/24: _____
- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZOR4 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZNER1 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 20.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZSER1 y contienen los atributos cluster-list y originator-ID, escriba el contenido de dichos atributos:

- 
- 20.0.0.0/24: _____
- 30.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZSER2 y contienen los atributos cluster-list y originator-ID, escriba el contenido de dichos atributos:

- 20.0.0.0/24: _____
- 30.0.0.0/24: _____
- 40.0.0.0/24: _____

## TAREA 3: Diseño y configuración de reflectores de ruta jerárquicos

**Paso 1:** Planeación y preparación de la red.

Se pueden construir clusters de reflectores de ruta en jerarquías, con lo cual un router que sirve como un reflector de ruta en un cluster puede actuar como un cliente en otro cluster.

Un router que está configurado para ser un reflector de ruta seguirá teniendo sesiones IBGP ordinarias que son parte de la malla completa. Si estas sesiones son reducidas en número y sólo quedan unas pocas, las restantes pueden alcanzar un segundo nivel de reflectores de ruta, y se creará una jerarquía de reflectores de ruta.[19]

Planee un diseño con reflectores de ruta, en donde construya un primer nivel de clusters para reducir el tamaño de la malla completa, y que la malla completa restante se pueda reducir al implementar un segundo nivel de reflectores de ruta.

**Paso 2:** Migración de la red.

Construya el diseño con reflectores de ruta jerárquicos. Para configurar un reflector de ruta como cliente en otro cluster, se utiliza el comando en modo de configuración de router:

**neighbor** rrclient-ip-*address* **route-reflector-client**

**Paso 3:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

¿Es posible realizar un ping desde la interfaz *Loopback* 0 del router AS200 a la interfaz *Loopback* 0 de los routers AS300, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback* 0 del router AS300 a la interfaz *Loopback* 0 de los routers AS200, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback* 0 del router AS400 a la interfaz

19 Cisco System Learning.Configuring BGP on Cisco Routers.Version 3.2. Volumen 2. Estados Unidos. 2005. p. 278.

*Loopback* 0 de los routers AS200, AS300 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback* 0 del router AS500 a la interfaz *Loopback* 0 de los routers AS200, AS300 y AS400? SI ___ NO ___

Si las siguientes redes, están presentes en la tabla BGP del router ZCR1 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 20.0.0.0/24: _____
- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

- Si las siguientes redes, están presentes en la tabla BGP del router ZCR3 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:
- 20.0.0.0/24: _____
- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZOR4 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 30.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZNER1 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 20.0.0.0/24: _____
- 40.0.0.0/24: _____
- 50.0.0.0/24: _____

Si las siguientes redes, están presentes en la tabla BGP del router ZSER1 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 20.0.0.0/24: _____
- 30.0.0.0/24: _____
- 50.0.0.0/24: _____

- Si las siguientes redes, están presentes en la tabla BGP del router ZSER2 y contienen los atributos ***cluster-list*** y ***originator-ID***, escriba el contenido de dichos atributos:

- 20.0.0.0/24: _____
- 30.0.0.0/24: _____
- 40.0.0.0/24: _____

# 6.5. LABORATORIO NO. 6.3 - CONFEDERACIONES

## 6.5.1. DIAGRAMA DE TOPOLOGÍA

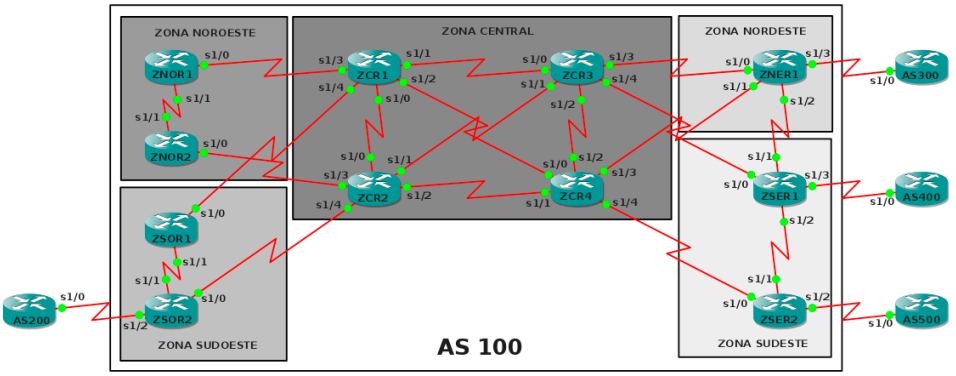


***Figura 6.3.*** Topología Confederaciones

## 6.5.2. TABLAS DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| ZCR1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| ZCR2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Loopback0 | | |
| ZCR3 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| ZCR4 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Serial 1/4 | | |
| | Loopback0 | | |
| ZNOR1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |
| ZNOR2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |
| ZSOR1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Loopback0 | | |
| ZSOR2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| ZNER1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Loopback 0 | | |
| ZSER1 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Serial 1/3 | | |
| | Loopback 0 | | |
| ZSER2 | Serial 1/0 | | |
| | Serial 1/1 | | |
| | Serial 1/2 | | |
| | Loopback 0 | | |

Tabla 6.4. Confederaciones [AS 100]

## 6.5.3. DESCRIPCIÓN DE LA ACTIVIDAD

## TAREA 1: Reestructuración y reconfiguración de la red

**Paso 1:** Reestructure la red para que sea similar a la del diagrama de la topología.

Con la red construida en el laboratorio de **reflectores de ruta jerárquicos** como base, reestructúrela como se indica en el diagrama de topología.

**Paso 2:** Reconfiguración de los dispositivos de la red.

Realice las configuraciones y modificaciones que considere pertinentes para que la red existente tenga un comportamiento similar al que se muestra en la topología. Tenga en cuenta el direccionamiento necesario para las interfaces de los routers añadidos a la red, y configurar en ellos el protocolo de enrutamiento dinámico OSPF bajo las mismas especificaciones mencionadas en el laboratorio de reflectores de ruta}.

Documente las direcciones a utilizarse en la tabla proporcionada debajo del diagrama de topología.

## TAREA 2: Configurar el enrutamiento BGP en cada uno de los ASs

**Paso 1:** Establecer sesiones IBGP.

**Consulte y analice:**

¿Cuántas sesiones IBGP se deberán establecer para configurar una malla completa al interior del AS 100?

_____

¿Cuántas sesiones IBGP se deberán establecer para configurar un diseño con reflectores de ruta?

_____

¿La topología cumple con todos los requisitos necesarios para implementar un diseño con reflectores de ruta? ¿Por qué?

_____

_____

_____

_____

Construya un diseño de malla completa con sesiones IBGP a partir de las interfaces *Loopback* de los router. Recuerde implementar el comando **next-hop-self** sobre los routers de borde de la red.

**Paso 2:** Establecer sesiones EBGP.

Restablezca sesiones EBGP entre ASs donde considere que sea necesario, recuerde que sólo se deben establecer entre los routers de borde entre interfaces directamente conectadas.

**Paso 3:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS200 a la interfaz *Loopback 0* de los routers AS300, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS300 a la interfaz *Loopback 0* de los routers AS200, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS400 a la interfaz *Loopback 0* de los routers AS200, AS300 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS500 a la interfaz *Loopback 0* de los routers AS200, AS300 y AS400? SI ___ NO ___

¿Qué rutas BGP están presentes en la tabla de BGP del router ZCR1?

¿Qué rutas BGP están presentes en la tabla de BGP del router ZCR2?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS200?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS300?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS400?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS500?

## TAREA 3: Diseño y configuración de confederaciones

Un gran número de routers en un AS de gran tamaño introducirá tradicionalmente una estructura de malla completa de sesiones IBGP compleja. Al dividir el AS en un determinado número de pequeños AS, la gran estructura compleja de sesiones IBGP se reducirá a estructuras IBGP bastante simples dentro de los pequeños sistemas. Las interconexiones entre estos AS podrían entonces ser realizadas utilizando EBGP, lo cual permitirá topologías arbitrarias.
Las **confederaciones BGP** están basadas en el concepto de que un AS puede dividirse en múltiples subAS. Dentro de cada subAS, se aplican todas las reglas de las sesiones IBGP. Todos los routers BGP dentro del subAS, por ejemplo, deben estar completamente en malla. Como cada subAS tiene un número de AS diferente, el BGP externo debe ejecutarse entre ellos. Aunque EBGP se usa entre los subAS, el enrutamiento dentro de la confederación se comporta como el enrutamiento IBGP dentro de un solo AS. En otras palabras, el próximo salto, MED, y la información de preferencia local se preserva al cruzar los límites del subAS. Para el mundo exterior, una confederación se asemeja a un solo AS.[20]

Los números AS que es usado dentro de la confederación nunca es visible desde fuera del AS, esto permite que puedan ser asignados números AS privados (en el rango 64.512 a 65.535) para identificar un subAS, sin necesidad de coordinar la asignación de números AS con una autoridad oficial de delegación de números AS.[21]

Entre *member-AS* dentro de una confederación, se establecen sesiones EBGP. Estas sesiones EBGP se comportan ligeramente diferente de las sesiones EBGP clásicas y son, por lo tanto, llamadas sesiones *EBGP intra-confederation* para diferenciarlas de las sesiones EBGP verdaderas.

**Consulte y analice:**

¿Cuáles son las diferencias entre las sesiones **EBGP clásicas** y las sesiones **EBGP intra-confederation**?
**Paso 1:** Planeación y preparación de la red.

Cuando se diseña confederaciones, se debe tener presente dos reglas básicas de diseño:

- No hay restricciones sobre sesiones EBGP intra-confederation.
- Sigue siendo necesario establecer una malla completa de sesiones IBGP dentro de cualquier member-AS

20 Cisco System Learning.Configuring BGP on Cisco Routers.Version 3.2. Volumen 2. Estados Unidos. 2005. p. 257.

21 Ibíd., p. 257.

**Nota:** Es recomendable un diseño de confederación centralizado, el cual conduce a un mejor desempeño. Diseño **centralizado** significa que todos los *member-AS* intercambiarán información de enrutamiento con cada uno de los otros *member-AS* a través de un **member-AS central** el cual funciona como *backbone* de la red.

Antes de migrar de una malla completa de sesiones IBGP a un diseño con confederaciones, es necesario realizar los siguientes preparativos:

- Identificar un grupo de routers de núcleo que puedan servir como member-AS central.
- Identificar varios grupos de routers más periféricos en los cuales, dentro de cada grupo, los routers estén bien conectados. Cada grupo conformará su propio member-AS.
- Realizar un plan de enumeración para asignar números AS privados (64.512 a 65.535) para los member-AS. El plan debe identificar de forma única a cada member-AS dentro de la confederación.
- Asegurarse que ningún router carece de soporte para implementar confederaciones. El software IOS de Cisco soporta esta función desde la versión 10.3.
- Remover la configuración BGP original con el número AS oficial.

**Paso 2:** Migración de la red.

Después de haber realizado los preparativos necesarios para migrar desde una malla completa de sesiones IBGP a un diseño con confederaciones, se necesitan completar los siguientes pasos:

- Realizar una nueva configuración de BGP que utilice el número de member-AS interno de acuerdo al plan de enumeración de AS para la confederación.
- Especificar el número de AS oficial original como el identificador de la confederación. Esta información será usada por los routers de borde de la confederación cuando se estén comunicando con otros AS externos.
- Especificar una lista de números de member-AS que estén en uso. El router utiliza esta información para distinguir entre comportamiento EBGP intra-confederation y comportamiento EBGP verdadero.
- Configurar todas las sesiones IBGP en la malla completa dentro de cada member-AS.
- Configurar sesiones EBGP intra-confederation entre member-AS de manera de que no se introduzcan puntos únicos de falla.
- Configurar sesiones EBGP verdaderas con AS externos.

**Paso 3:** Verificar las configuraciones y la conectividad.

Revise el estado del proceso de BGP y de las sesiones entre vecinos.

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS200 a la interfaz *Loopback 0* de los routers AS300, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS300 a la interfaz *Loopback 0* de los routers AS200, AS400 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS400 a la interfaz *Loopback 0* de los routers AS200, AS300 y AS500? SI ___ NO ___

¿Es posible realizar un ping desde la interfaz *Loopback 0* del router AS500 a la interfaz *Loopback 0* de los routers AS200, AS300 y AS400? SI ___ NO ___

¿Qué rutas BGP están presentes en la tabla de BGP del router ZCR1?

¿Qué rutas BGP están presentes en la tabla de BGP del router ZCR2?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS200?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS300?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS400?

¿Qué rutas BGP están presentes en la tabla de enrutamiento del router AS500?

# SEGUNDA PARTE LABORATORIOS MPLS
# 1. LABORATORIO N° 1- MPLS MODO TRAMA

## 1.1. INTRODUCCIÓN

El modo de operación MPLS se puede clasificar en dos categorías de acuerdo a la forma de asignar y codificar la etiqueta en un paquete IP: MPLS modo trama y MPLS modo celda. En MPLS modo trama cada router asigna e inserta una etiqueta entre el encabezado de la trama de capa 2 y el encabezado del paquete de capa 3.[22]

Este laboratorio está orientado comprender de forma precisa los conceptos fundamentales de MPLS modo trama y todos los procesos de asignación, distribución y modos de retención de etiquetas involucrados.

## 1.2. OBJETIVOS

Al completar esta práctica de laboratorio usted podrá:

- Habilitar la conmutación CEF.
- Configurar el MPLS ID en un router.
- Configurar MPLS en una interfaz en modo trama.
- Establecer el campo MTU por interface para los paquetes etiquetados.
- Configurar la propagación IP TTL.
- Configurar la distribución condicional de etiqueta.
- Monitorear el funcionamiento de MPLS en la red.

22 ARIGANELLO, Ernesto; BARRIENTOS, Ernesto. REDES CISCO. CCNP a fondo. Guía de estudio para profesionales. Primera Edición. Alfaomega Grupo Editor. México. 2010. p. 575

## 1.3. DIAGRAMA DE LA TOPOLOGÍA

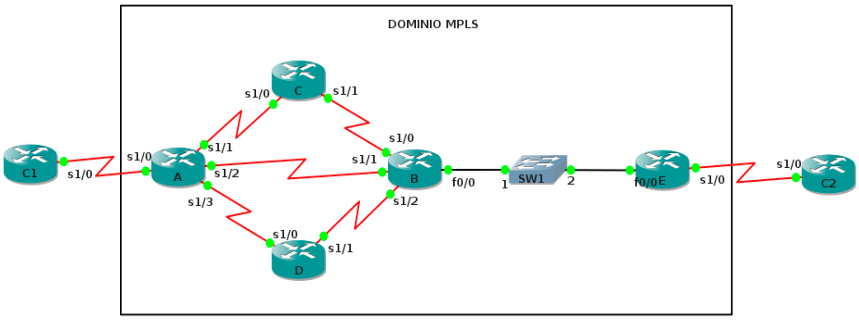


***Figura 1.1.*** Topología MPLS modo trama

## 1.4. TABLA DE DIRECCIONAMIENTO GENERAL

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| A | S1/0 | | |
| | S1/1 | | |
| | S1/2 | | |
| | S1/3 | | |
| | Lo0 | | |
| B | Fa0/0 | | |
| | S1/0 | | |
| | S1/1 | | |
| | S1/2 | | |
| | Lo0 | | |
| C | S1/0 | | |
| | S1/1 | | |
| | Lo0 | | |
| D | S1/0 | | |
| | S1/1 | | |
| | Lo0 | | |
| E | Fa0/0 | | |
| | S1/0 | | |
| | Lo0 | | |

| | | | |
|---|---|---|---|
| C1 | S1/0 | | |
| | Lo0 | | |
| | Lo1 | | |
| | Lo2 | | |
| | Lo3 | | |
| C2 | S1/0 | | |
| | Lo0 | | |
| | Lo1 | | |
| | Lo2 | | |
| | Lo3 | | |

Tabla 1.1 MPLS modo trama

## 1.5. DESCRIPCIÓN DE LA ACTIVIDAD

### TAREA 1: Diseñar y documentar un esquema de direccionamiento

**Paso 1:** Diseñe un esquema de direccionamiento.

Utilice la topología mostrada previamente y diseñe el esquema de direccionamiento con base en los siguientes requisitos:

Para las conexiones al interior del dominio MPLS establezca las conexiones de acuerdo a la siguiente tabla utilizando la subred 172.255.0.0/27.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| A <> C | 0 | | |
| A <> B | 1 | | |
| A <> D | 2 | | |
| C <> B | 3 | | |
| D <> B | 4 | | |
| B <> E | 5 | | |

Para las conexiones entre C1, C2 y la red MPLS establezca las conexiones de acuerdo a la siguiente tabla utilizando la subred 192.168.0.0/28.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| C1 <> A | 0 | | |
| C2 <> E | 1 | | |

**Paso 2:** Documente el esquema de direccionamiento.

Documente las direcciones IP y máscaras de subred con la ayuda de las tablas proporcionadas.

## TAREA 2: Preparación básica de la red

**Paso 1:** Conecte una red que sea similar a la del diagrama de topología.

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en el gráfico.

**Paso 2:** Configuración básica de los enrutadores.
Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautas generales (utilice como contraseña la palabra *"nyquist"*):

1. Configure el nombre de host del router.
2. Configure una contraseña de modo EXEC privilegiado.
3. Configure un mensaje del día.
4. Configure una contraseña para las conexiones de la consola.
5. Configure una contraseña para las conexiones de VTY.

## TAREA 3: Configurar el enrutamiento dinámico en el dominio MPLS

Configure el enrutamiento OSPF (proceso ID 1) en cada router del dominio MPLS.

## TAREA 4: Establezca la conexión entre C1 y C2

**Paso 1:** Lleve a cabo la conexión entre C1 y C2 a través de la red MPLS mediante enrutamiento estático.

**Paso 2:** Asegúrese que la conexión entre C1 y C2 se halla establecido. De no ser así solucione el problema.

## TAREA 5: Configurar IP CEF

Explique el mecanismo de conmutación **process switching** señalando sus ventajas y desventajas

_____
_____
_____
_____
_____.

Explique el mecanismo de conmutación **cache-driven switching** señalando sus ventajas y desventajas

_____
_____
_____
_____
_____.

Habilite la conmutación CEF en cada uno de los routers de la topología mediante el comando de configuración global **ip cef** [**distributed**].

Nota: El mecanismo de conmutación CEF está habilitado por defecto en las plataformas cisco 7100, 7200, 7500, 6500 y 12000.

## TAREA 6: Configurar MPLS en las interfaces modo trama

Mientras que un protocolo de enrutamiento IP intercambia información de enrutamiento y mantiene la tabla de enrutamiento IP a través de una red de datos, un protocolo de distribución de etiquetas se encarga del intercambio de información de mapeo de etiquetas en un entorno MPLS.[23]

A cada dirección de red presente en la tabla de enrutamiento IP (FEC) se asigna una etiqueta con significado a nivel local. Con base en esta información se crea una nueva estructura de datos denominada LIB (Label Information Base). En cada LSR en el dominio MPLS el protocolo de distribución de etiquetas crea dicha tabla y anuncia esta información a sus vecinos adyacentes.

A partir de la información recibida y generada a nivel local cada LSR en la red completa las tablas LIB y FIB (creada previamente mediante CEF) y crea una base de datos adicional, la tabla LFIB (Label Forwarding Information Base).[24]

23 ARIGANELLO, Ernesto; BARRIENTOS, Ernesto. REDES CISCO. CCNP a fondo. Guía de estudio para profesionales. Primera Edición. Alfaomega Grupo Editor. México. 2010. p. 577.

24 ARIGANELLO, Ernesto; BARRIENTOS, Ernesto. REDES CISCO. CCNP a fondo. Guía de estudio para profesionales. Primera Edición. Alfaomega Grupo Editor. México. 2010. p. 577.

La LIB mantiene el enlace entre los prefijos IP, la etiqueta asignada a nivel local y la etiqueta de siguiente salto. La FIB contendrá cada dirección IP con la dirección de siguiente salto respectiva asociado a la etiqueta de salida y la LFIB contendrá un mapeo completo entre la etiqueta local y la etiqueta de siguiente salto generada para cada prefijo IP. De este modo un paquete puede ser enrutado o conmutado por etiquetas de acuerdo a la información presente en las tablas FIB Y LFIB.[25]

De acuerdo a esta información:

Describa el proceso de conmutación IP para un paquete que ingresa en el dominio MPLS.
_____
_____
_____
_____
_____
_____.
Describa el proceso de conmutación IP efectuado por un LSR para un paquete etiquetado.
_____
_____
_____
_____
_____
_____.

**Paso 1:** Habilite la propagación de etiquetas mediante el protocolo de distribución de etiquetas adecuado.
En cada uno de los routers de la topología, habilite la conmutación de etiquetas en las interfaces adecuadas. Para llevar a cabo esta tarea utilice los comandos de configuración de interfaz **mpls ip** y **mpls label protocol** [**tdp**] [**ldp**] [**both**].

Nota: Tenga en cuenta que TDP es el protocolo de distribución de etiquetas desarrollado por cisco y no funciona en otro tipo de plataformas. LDP es el protocolo estándar y puede ser ejecutado en cualquier plataforma.

**Paso 2:** Establezca listas de control de acceso en los LSR de borde para bloquear las publicaciones TDP o LDP.

Cree listas de acceso en las interfaces adecuadas de los LSR de borde para bloquear el intento de establecimiento de sesión LDP o TDP. Tenga en cuenta que LDP utiliza los puertos TCP/UDP 711 mientras que TDP utiliza los puertos TCP/UDP 646.[26]

25 Ibíd., p. 577.

26 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p.152.

## TAREA 7: Modificar el tamaño máximo de los paquetes etiquetados

Defina MTU (Maximum Transfer Unit)

_____
_____
_____
_____.

El mecanismo MPLS podría suponer un exceso de tamaño de la MTU en las interfaces debido al agregado de una o más etiquetas a los paquetes que fluyen por la red. Este es tipo de problema es el más habitual al momento de llevar a cabo el despliegue de redes MPLS. Este problema puede generar la fragmentación de los paquetes que fluyen a través de la red.[27]

Para que los paquetes fluyan a través de la red de forma normal y sin presentase la fragmentación de los mismos es necesario adaptar la MTU para cada interfaz al tamaño correcto acorde al incremento que supone el agregado de etiquetas. Siempre se aconseja un tamaño MTU de 1512 bytes o superior.[28]

Establezca la MTU por interface con el valor adecuado para los paquetes etiquetados en cada uno de los routers de la red a través del comando de configuración de interfaz **mpls mtu** *bytes*.

Nota: El tamaño MTU MPLS se incrementa de forma automática en interfaces WAN, pero debe ser incrementado manualmente en interfaces LAN.

## TAREA 8: Configurar el MPLS ID

Antes de que cada LSR al interior del dominio MPLS distribuya la información presente en su tabla LIB se debe establecer relaciones de vecindad con sus pares a través de la red. El establecimiento de estas adyacencias se logra al generar sesiones LDP o TDP. Para que dichas sesiones tengan lugar se debe llevar a cabo un intercambio de mensajes HELLO entre los dispositivos de enrutamiento, de este modo los routers habilitados para MPLS responden a los mensajes HELLO recibidos intentando establecer una sesión con el origen de dichos mensajes. Esta dirección de origen es el número que identifica de forma exclusiva a cada router al interior en la red.[29]

Para especificar la interfaz preferida para determinar el router ID LDP utilice el comando **mpls ldp router-id** *interface* [**force**] en el modo de configuración global. Asegúrese que cada router en la red MPLS utilice la dirección de su interface loopback 0 como identificador.

27 Ibíd., p. 190.

28 Ibíd., p. 191.

29 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 152

## TAREA 9: Describir el proceso de propagación IP TTL a través del dominio de red

El protocolo de distribución de etiquetas depende de los mecanismos de prevención de loop incorporados en el IGP. Usualmente las rutas IP generadas a partir del IGP son rutas libres de bucles. Sin embargo un loop de paquetes etiquetados podría llegar a presentarse.

Al igual que el encabezado IP, el encabezado de la etiqueta cuenta con un campo TTL (Time-To-Live). Este campo tiene una funcionalidad equivalente al campo TTL del método de reenvió IP tradicional al evitar que el flujo de paquetes etiquetados entre en un loop indefinido.[30]
El campo TTL de la etiqueta puede establecerse de dos formas diferentes: Por defecto cuando un paquete es etiquetado, el campo TTL del encabezado IP se copia en el campo TTL del encabezado de la etiqueta y cuando se elimina la etiqueta el valor presente en el campo TTL de la etiqueta se copia de nuevo en el campo TTL del encabezado IP. A este proceso se le denomina **propagación TTL**. Cuando se deshabilita dicho proceso, el campo TTL IP no se copia en campo TTL de la etiqueta, en su lugar, el campo TTL en el encabezado de la etiqueta se establece al valor 255 de forma predeterminada. Cuando el paquete etiquetado atraviesa un LSR de borde de egreso la etiqueta se elimina y el valor TTL de la etiqueta no es copiado de nuevo en el campo TTL IP.[31]

Describa el funcionamiento de la función **traceroute**

_____
_____
_____
_____
_____
_____.

Ejecute el comando **tracert** desde C1 para determinar la ruta para el flujo de tráfico a través del de la red MPLS hacial C2. Describa este proceso de forma detallada. _____
_____
_____
_____
_____
_____.

30 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 184.

31 Ibíd., p. 184.

Deshabilite la **propagación ttl** en los router LSR de borde de la red MPLS y ejecute de nuevo el comando **tracert** desde C1 hacia C2. Describa el proceso. ¿Qué routers de la red generaron una respuesta ICMP a C1?, ¿A qué se debe este resultado?

_____
_____
_____
_____
_____
_____.

Después haber respondido estos dos interrogantes analice que posibles problemas puede suponer para una red MPLS que sus LSR de borde tengan habilitada la función **propagación ttl**

_____
_____
_____
_____
_____.

Deshabilite la función **ip ttl propagation** en los routers pertinentes de la red de manera que el administrador de red pueda llevar a cabo pruebas y resolver problemas mediante la función **traceroute** manteniendo oculta la estructura de red a los dispositivos externos**.**

Para ejecutar las tareas de configuración solicitadas en este apartado utilice los siguientes comandos con los parámetros adecuados en el modo de configuración global:

- mpls ip propagate-ttl [forwarded][local]
- no mpls ip propagate-ttl [forwarded][local]

## TAREA 10: Configurar la propagación condicional de etiqueta

Como se mencionó anteriormente, por defecto cada LSR en la red asigna de forma independiente una etiqueta a cada FEC (Forwarding Equivalence Class) y posteriormente consigna esta información en una estructura de datos llamada LIB. A este método de asignación de se conoce como **independent control mode.** Después de ejecutarse este proceso cada LSR anuncia de forma asíncrona la información presente en su tabla LIB a todos los vecinos adyacentes. Cada LSR construye sus tablas LIB, FIB y LFIB con base en la información recibida y generada a nivel local. Este proceso de distribución de etiquetas se denomina **unsolicited downstream distribution**.[32]

32 ARIGANELLO, Ernesto; BARRIENTOS, Ernesto. REDES CISCO. CCNP a fondo. Guía de estudio para profesionales. Primera Edición. Alfaomega Grupo Editor. México. 2010. p. 581

Ciertos escenarios podrían requerir anunciar de forma selectiva solo algunas etiquetas a un grupo específico de vecinos. De este modo los métodos de asignación y distribución predeterminados de etiquetas podrían no ser adecuados. Sin embargo, las plataformas cisco cuentan con un mecanismo para modificar los procesos antes mencionados.

**Paso 1:** Bloquee la distribución de etiquetas.

Asegúrese que el proceso distribución de etiquetas se lleve a cabo solo para las redes de C1 y C2. Para controlar el proceso de asignación e intercambio de etiquetas utilice el comando **mpls ldp advertise-labels** [**for** prefix-access-list] [**to** peer-access-list] en el modo de configuración global.

## TAREA 11: Asegúrese que se establecieron las configuraciones de forma correcta

- Asegúrese de haber establecido de forma correcta la configuración MPLS en las interfaces adecuadas de cada uno de los routers cisco de la red mediante el comando de show mpls interfaces [interface][detail].
- Supervise el estado del proceso de descubrimiento LDP mediante el comando show mpls ldp discovery.
- Asegúrese de haber generado las adyacencias de forma correcta mediante el comando show mpls ldp neighbor [vrf vpn-name][address][interface][detail][all]
- Asegúrese que el contenido de la tabla LIB para cada uno los routers cisco sea el correcto.Utilice el comando show mpls ldp bindings [vrf vpn-name] [network {mask|length} [longer-prefixes]] [local-label label[label]][remote-label label[-label]] [neighbor address ][local]
- Asegúrese que el contenido de la tabla LFIB para cada uno los routers cisco sea el correcto. Utilice el comando show mpls forwarding-table [network {mask|length} | labels label[label] | interface interface | next-hop address | lsp-tunnel [tunnel-id]] [detail]
- Asegúrese que el contenido de la tabla FIB para cada uno los routers cisco sea el correcto. Utilice el comando show ip cef [unresolved|summary]

# 2. LABORATORIO N° 2 - MPLS MODO CELDA

## 2.1. INTRODUCCIÓN

Como se mencionó en el escenario anterior, el modo de operación MPLS se puede categorizar de acuerdo a la forma de asignar y codificar la etiqueta en un paquete IP en dos tipos de ejecución: MPLS modo trama y MPLS modo celda. MPLS modo celda es radicalmente diferente al modo MPLS modo trama.

MPLS modo celda se ejecuta únicamente en entornos ATM. Este tipo de tecnología de transmisión utiliza celdas en lugar de tramas. Las celdas son estructuras de datos de longitud fija producto de la segmentación de paquetes. Debido a que las celdas tienen una longitud fija no es posible llevar a cabo el proceso de asignación de etiquetas. Como solución alternativa MPLS modo trama utiliza el valor presente en el campo VPI/VCI del encabezado ATM para codificar el valor de la etiqueta.[33]

Este laboratorio está orientado a comprender de forma precisa los conceptos fundamentales de MPLS modo celda y todos los parámetros de distribución asociados.

## 2.2. OBJETIVOS

- Enumerar las tareas de configuración de MPLS en interfaces LC-ATM.
- Describir los parámetros adicionales que pueden ser configurados en una interfaz LC-ATM.
- Monitorear el funcionamiento de LC-ATM MPLS.

33 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 116.

## 2.3. DIAGRAMA DE TOPOLOGÍA

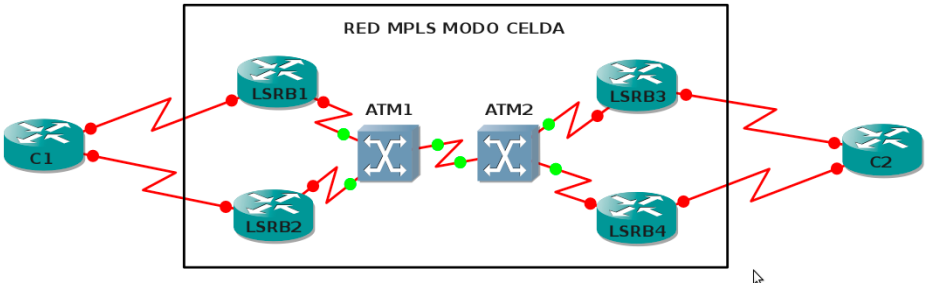


***Figura 2.1.*** Topología MPLS modo celda

## 2.4. TABLA DE DIRECCIONAMIENTO GENERAL

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| LSR-B1 | S0/0 | | |
| | atm 0/0.1 | | |
| | Lo0 | | |
| LSR-B2 | S0/1 | | |
| | atm 0/0.1 | | |
| | Lo0 | | |
| LSR-B3 | S0/0 | | |
| | atm 0/0.1 | | |
| | Lo0 | | |
| LSR-B4 | S0/0 | | |
| | atm 0/0.1 | | |
| | Lo0 | | |
| SW1 | atm 0/0.1 | | |
| | atm 0/0.2 | | |
| | atm 0/0.3 | | |
| SW1 | atm 0/0.1 | | |
| | atm 0/0.2 | | |
| | atm 0/0.3 | | |

| | | | |
|---|---|---|---|
| C1 | S0/0 | | |
| | Lo0 | | |
| | Lo1 | | |
| | Lo2 | | |
| | Lo3 | | |
| C2 | S0/0 | | |
| | Lo0 | | |
| | Lo1 | | |
| | Lo2 | | |
| | Lo3 | | |

Tabla 2.1. AS de Tránsito

## 2.5. DESCRIPCIÓN DE LA ACTIVIDAD

### TAREA 1: Diseñar y documentar un esquema de direccionamiento

**Paso 1:** Diseñe un esquema de direccionamiento.

Utilice la topología mostrada previamente y diseñe el esquema de direccionamiento con base en los siguientes requisitos:

Para las conexiones al interior del dominio MPLS, establezca las conexiones de acuerdo a la siguiente tabla utilizando la subred 172.255.0.0/27.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| LSR-B1 <> SW1 | 0 | | |
| LSR-B2 <> SW1 | 1 | | |
| LSR-B3 <> SW2 | 2 | | |
| LSR-B4 <> SW2 | 3 | | |
| SW1 <> SW2 | 4 | | |

Para las conexiones entre C1 y C2 y la red MPLS, establezca las conexiones de acuerdo a la siguiente tabla utilizando la subred 192.168.0.0/28.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| C1 <> LSR-B1 | 0 | | |

| | | | |
|---|---|---|---|
| C1 <> LSR-B2 | 1 | | |
| C2 <> LSR-B3 | 2 | | |
| C2 <> LSR-B4 | 3 | | |

## TAREA 2: Aplicar una configuración básica

**Paso 1:** Conecte una red que sea similar a la del diagrama de topología.

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en el gráfico.

**Paso 2:** Configuración básica de los enrutadores.

Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautas generales (utilice como contraseña la palabra *"nyquist"*):

1. Configure el nombre de host del router.
2. Configure una contraseña de modo EXEC privilegiado.
3. Configure un mensaje del día.
4. Configure una contraseña para las conexiones de la consola.
5. Configure una contraseña para las conexiones de VTY.

## TAREA 3: Configurar el enrutamiento dinámico en el dominio MPLS

Configure el enrutamiento OSPF (proceso ID 1) en cada router del dominio MPLS.

## TAREA 4: Establezca la conexión entre C1 y C2

**Paso 1:** Lleve a cabo la conexión entre C1 y C2 a través de la red MPLS mediante enrutamiento estático.

**Paso 2:** Asegúrese que la conexión entre C1 y C2 se halla establecido. De no ser así solucione el problema.

## TAREA 5: Configurar IP CEF

Como se explicó en el laboratorio anterior, existen tres mecanismos de conmutación soportados por las plataformas cisco: **process switching**, **cache-driven switching** y **topology-driven switching (CEF)**. Para que MPLS funcione de manera correcta independientemente

del modo de ejecución, es necesario configurar de forma previa el mecanismo de conmutación **CEF (Cisco Express Forwarding).**[34]

Habilite la conmutación CEF en cada uno de los routers de la topología mediante el comando de configuración global **ip cef** [**distributed**].

Nota: El mecanismo de conmutación CEF está habilitado por defecto en las plataformas cisco 7100, 7200, 7500, 6500 y 12000.

## TAREA 6: Configurar MPLS en las interfaces modo celda

Al igual que en MPLS modo trama, MPLS modo celda ejecuta un protocolo de enrutamiento IP y un protocolo de distribución de etiquetas en el plano de control. La diferencia primordial de estos dos modos de ejecución radica en la forma en que ambos llevan a cabo el proceso de asignación y distribución de etiquetas y la forma en que las estructuras de datos LIB, FIB y LFIB son pobladas con la información obtenida mediante los protocolos nombrados previamente.

En MPLS modo trama las etiquetas tienen que ser explícitamente solicitadas a través de las interfaces LC-ATM puesto que un LSR asignará una etiqueta a un prefijo solo si recibe una solicitud de un vecino ascendente para dicha etiqueta. De este modo cada LSR ATM en el dominio MPLS solicita una etiqueta para cada FEC en su tabla IP desencadenando una secuencia ordenada de solicitudes descendentes de etiqueta a lo largo de la red. Este mecanismo de distribución de etiquetas se denomina **Downstream-on-demand.** Dicho proceso es generado debido a que en un entorno ATM MPLS un LSR puede asignar una etiqueta solo si ya ha recibido la etiqueta correspondiente del LSR de siguiente salto, de otra forma el LSR debe solicitar la etiqueta respectiva a dicho vecino. De este modo el proceso de solicitud de etiquetas termina solo cuando la etiqueta de salida está disponible o cuando la solicitud supera el dominio modo celda; es decir, cuando la solicitud alcanza un LSR que tenga una etiqueta de siguiente salto asignada o cuando la solicitud llegue a un LSR de borde ya que este tipo de dispositivo utiliza un modo de control independiente. Si se satisface uno de estos dos requisitos se produce un proceso denominado **ordened control mode** que desencadena una secuencia ordenada de respuestas ascendentes para las solicitudes recibidas previamente.[35][36]

En resumen, en un entorno MPLS ATM los procesos de propagación y asignación de etiquetas se combinan dando lugar a una secuencia descendente de solicitudes seguido de un proceso en cascada de respuestas ascendentes.

34 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 174.

35 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 142

36 Ibíd. p. 143

De acuerdo a este modo de operación:

Describa de forma detallada el proceso mediante el cual se llena la tabla LIB

_____
_____
_____
_____
_____
_____.

Describa de forma detallada el proceso mediante el cual se llena la tabla FIB

_____
_____
_____
_____
_____
_____.

Describa de forma detallada el proceso mediante el cual se llena la tabla LFIB

_____
_____
_____
_____
_____
_____.

Al igual que MPLS modo trama, MPLS modo celda cuenta con dos tipos de dispositivos que ejecutan funciones particulares en el dominio MPLS: los LSR núcleo y los LSR de borde. Estos dispositivos reciben estos nombres debido a la posición que ocupan en la red.[37]

En el contexto ATM Los LSR de borde se denominan LRSs ATM de borde y se ubican en la periferia de la red. Estos dispositivos se ocupan de segmentar los paquetes recibidos en celdas y reenviarlas en el dominio MPLS, o re ensamblar las celdas en paquetes y reenviarlos fuera de la red MPLS. Por otra parte los LSR núcleo reciben el nombre de LSR ATM. Estos artefactos se ubican en el centro de la red y sus funciones están limitadas al reenvío de celdas etiquetadas.[38]

Nota: Generalmente las funciones de un LSR ATM de borde son ejecutadas por un router, mientras que las funciones de un LSR ATM están a cargo de un SWITCH ATM.

37 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 36.

38 Ibíd., p. 37.

De acuerdo a esta información:

Describa el proceso de conmutación IP para un paquete que ingresa en el dominio ATM-MPLS.

_____
_____
_____
_____
_____.

Describa el proceso de conmutación IP efectuado por un LSR-ATM para una celda.

_____
_____
_____
_____
_____.

**Paso 1:** Configure las interfaces LC-ATM respectivas en los LSR ATM de borde.

- En cada uno de los LSR ATM de borde cree las subinterfaces LC-ATM respectivas mediante el comando interface atm number.sub-number mpls. La palabra clave mpls se utiliza para especificar que el MPLS modo celda será utilizado.

- En cada uno de los LSR ATM de borde de la topología, habilite la conmutación de etiquetas en las interfaces adecuadas. Para llevar a cabo esta tarea utilice los comandos de configuración de interfaz mpls ip y mpls label protocol [tdp] [ldp] [both].

**Paso 2:** Configure las interfaces LC-ATM respectivas en los switches ATM de la red.

Los switches ATM a diferencia de los conmutadores tradicionales pueden ejecutar un protocolo de enrutamiento y generar una tabla de enrutamiento a partir de la información obtenida mediante dicho protocolo.[39]

En el plano de control cada switch ATM actúa como un router IP, de este modo las tablas de enrutamiento IP se construyen como si los switches ATM fuesen routers.[40]

Debido a que los switches ATM actúan como un router IP, son vistos como un salto extra en la red IP. Sin embargo, los switches ATM no pueden reenviar paquetes IP ya que estos dispositivos no pueden realizar búsquedas en la tabla de enrutamiento.[41]

39 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 28.

40 Ibíd., p. 39.

41 Ibíd, p. 50.

**¿Por qué los switches ATM no pueden realizar búsquedas en la tabla de enrutamiento?**

_____
_____
_____
_____
_____.

En cada uno de los switches ATM cree las subinterfaces LC-ATM respectivas mediante el comando **interface atm** number.

En cada uno de los switches ATM de la topología, habilite la conmutación de etiquetas en las subinterfaces adecuadas. Para llevar a cabo esta tarea utilice los comandos de configuración de interfaz **mpls ip** y **mpls label protocol** [**tdp**] [**ldp**] [**both**].

**Paso 3:** Establezca listas de control de acceso en los LSR de borde para bloquear las publicaciones TDP o LDP.
Cree listas de acceso en las interfaces adecuadas de los LSR de borde para bloquear el intento de establecimiento de sesión LDP o TDP. Tenga en cuenta que LDP utiliza los puertos TCP/UDP 711 mientras que TDP utiliza los puertos TCP/UDP 646.

## TAREA 7: Establezca la configuración adicional de los parámetros LC-ATM. (Opcional)

Antes de que cada LSR al interior del dominio MPLS distribuya la información presente en su tabla LIB se debe establecer relaciones de vecindad con sus pares a través de la red. El establecimiento de estas adyacencias se logra al generar sesiones LDP o TDP. En un entorno ATM los ATM LSRs generan adyacencias mediante el circuito virtual de control MPLS. Este campo por defecto tiene un valor VPI/VCI igual a 0/32. Este circuito de control es utilizado por el protocolo de enrutamiento IP y el protocolo de distribución de etiquetas para el intercambio de información. Cuando se establece la adyacencia mediante el protocolo de distribución de etiquetas los dispositivos inician la negociación de los LVC (label-swited controlled Virtual Circuit).[42]

Use el comando de configuración de interfaz **mpls atm control-vc** *vpi* vci para modificar los valores de la tupla VPI/VCI utilizado para establecer el enlace inicial utilizado para establecer la sesión LDP.

42 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 158.

**¿Bajo qué circunstancias en necesario modificar los valores VPI/VCI por defecto utilizados para establecer el circuito virtual de control?**

_____
_____
_____
_____.

Use el comando de configuración de interfaz **mpls atm vpi** *vpi* [- *vpi*] para configurar el rango de valores que serán utilizados en el campo VPI para los LVCs.

**¿Bajo qué circunstancias en necesario configurar el rango de valores que serán utilizados en el campo VPI para los LVCs?**

_____
_____
_____
_____.

## TAREA 8: Describir el proceso de detección de loops en una red MPLS ATM

El encabezado de la celda ATM utiliza los campos VPI/VCI para identificar el circuito virtual ATM. Debido a las limitaciones de la arquitectura ATM, MPLS modo celda debe utilizar estos campos para codificar el valor de la etiqueta en lugar de agregar una etiqueta real. Estos campos no contienen el valor TTL. Por tanto, MPLS modo celda debe utilizar otro tipo de mecanismos para prevenir los loops de enrutamiento.[43]

El protocolo de distribución de etiquetas utiliza un campo TLV (tipo, longitud, valor) para contar el número de saltos en un LSP. Los LSR de borde además de propagar la dupla prefijo IP-etiqueta determinan la longitud de cada LSP generado a través del dominio ATM mediante el conteo de los saltos que componen cada circuito virtual. Cuando un paquete llega al dominio ATM el campo TTL del paquete es decrementado por el TLV específico.[44]

Investigue de que forma el campo TLV es utilizado para evitar loops de enrutamiento. ____
_____
_____
_____
_____.

43 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 127.

44 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 128.

¿De acuerdo a la topología cual debe ser el número de saltos permitidos en el LSP establecido? ¿Por qué?

_____
_____
_____
_____.

Establezca el número de saltos adecuado mediante el comando de configuración global **mpls ldp maxhops** *number*

## TAREA 9: Resolver el problema cell interleaving

ATM utiliza los valores VPI/VCI por interface, en consecuencia MPLS modo celda a diferencia de MPLS modo trama asigna una etiqueta para cada FEC en la tabla de enrutamiento por cada una de las interfaces del dispositivo. Este comportamiento hace que para una red en la tabla de enrutamiento IP se creen múltiples etiquetas en entrada ligadas directamente al número de interfaces involucradas en el proceso de conmutación. Este tipo de asignación de etiqueta se denomina **per-interface label allocation.** Dicho proceso está determinado por el número de sesiones descendentes establecidas, vinculando una etiqueta de origen local diferente a cada sesión independiente para cada prefijo ip.[45]

¿Qué ventaja representa el proceso **per-interface label allocation**?

_____
_____
_____
_____.

En una red MPLS ATM cada LSR descendente solicitará a un LSR ascendente una etiqueta por cada uno de los destinos descendentes. Este comportamiento puede llegar a generar que múltiples enlaces virtuales se yuxtapongan en un único enlace desencadenando una mezcla de etiquetas a través de un solo canal.

¿De acuerdo a la arquitectura de ATM qué problemas puede generar el **cell interleavin**?

_____
_____
_____
_____
_____.

45 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p.133.

Existen dos alternativas para evitar la mezcla de etiquetas a través de un solo enlace:

**Solucion1: Asignar una etiqueta downstream independiente por cada solicitud upstream.**

En este escenario los LSR ATM solicitan una nueva etiqueta de los LSRs descendentes por cada solicitud ascendente, los routers de egreso tiene que asignar una etiqueta única para cada ATM de entrada por cada destino. Este proceso crea un túnel LSP adicional para la misma red de destino por cada upstream ATM edge LSR.[46]

Señale ventajas y desventajas de este método

_____
_____
_____
_____
_____.

**Solución2: Las celdas entrantes son bloqueadas hasta que la última celda en una trama llega.**

En este esquema se almacena temporalmente las celdas del segundo paquete hasta que las celdas del primer paquete sean reenviadas. Posteriormente todas las celdas almacenadas son enviadas al ATM LSR de siguiente salto. Este mecanismo se denomina **VC merge.**[47]

Señale ventajas y desventajas del método VC merge

_____
_____
_____
_____
_____.

Es posible asegurar que mediante este modo de operación la red ATM es transformada en una red
MPLS modo trama? Si no ¿Por qué?

_____
_____
_____
_____
_____.

46 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004., p. 124.

47 Ibíd., p. 125.

¿Por qué las etiquetas en MPLS modo celda son un recurso escaso?

_____
_____
_____
_____
_____.

Nota: VC merge está habilitado por defecto en todos los dispositivos que soporten esta funcionalidad.

¿Bajo qué circunstancias en necesario deshabilitar la función VC merge?

_____
_____
_____
_____.

## TAREA 10: Configurar la propagación condicional de etiqueta

Como se mencionó anteriormente, los procesos de asignación y distribución de etiquetas se conjugan dando lugar a una cascada de solicitudes ascendentes seguida de una secuencia ordenada de respuestas descendentes para cada una de las solicitudes previas.

Bajo ciertas circunstancias podría ser necesario ejecutar los procesos de asignación y distribución de etiquetas anunciando de forma selectiva solo algunas etiquetas a determinados vecinos de la red.

**Bloquee la distribución de etiquetas.**

Asegúrese que el proceso distribución de etiquetas se lleve a cabo solo para las redes de C1 y C2. Para controlar el proceso de asignación e intercambio de etiquetas utilice el comando **mpls ldp request-tags for** en el modo de configuración global.

## TAREA 11: Asegúrese que se establecieron las configuraciones de forma correcta

- Asegúrese de haber establecido de forma correcta la configuración MPLS en las interfases adecuadas de cada uno de los routers cisco de la red mediante el comando de show mpls

- Supervise el estado del proceso de descubrimiento LDP mediante el comando show mpls

- Asegúrese de haber generado las adyacencias de forma correcta mediante el comando show mpls
- Asegúrese que el contenido de la tabla LIB para cada uno los routers cisco sea el correcto.Utilice el comando show mpls
- Asegúrese que el contenido de la tabla LFIB para cada uno los routers cisco sea el correcto.Utilice el comando show mpls
- Asegúrese que el contenido de la tabla FIB para cada uno los routers cisco sea el correcto. Utilice el comando show ip cef [unresolved|summary]

# 3. LABORATORIO N° 3 – IMPLEMENTANDO MPLS VPN

## 3.1. INTRODUCCIÓN

MPLS (Multiprotocol Label Switching) VPN (Virtual Private Network) es la implementación más popular y extensa de MPLS. Aunque la mayoría de los proveedores de servicios la han implementado como un reemplazo para los servicios Frame Relay y ATM, las grandes empresas están teniendo un gran interés por implementar MPLS VPN como el próximo paso en el diseño de red. MPLS VPN puede proporcionar escalabilidad y segmentación de la red global en redes más pequeñas e independientes entre sí, lo cual generalmente es necesario en redes empresariales grandes, donde la infraestructura de TI común tiene que ofrecer redes aisladas para los distintos departamentos de la empresa. Muchos proveedores de servicios, que han implementado MPLS VPN durante años, ahora están buscando interconectar su red a las redes MPLS VPN de otros proveedores de servicios para mejorar la escalabilidad y la facilidad de uso de su red.[48]

Una VPN es una red que emula una red privada sobre una infraestructura común, que puede proporcionar una comunicación a nivel de capa 2 ó de capa 3 del modelo OSI. Generalmente se asigna una VPN a una empresa, con el objetivo de interconectar varios sitios o sucursales a través de la infraestructura de un proveedor de servicio. Los requisitos mínimos de conectividad para una red privada incluyen la interconexión entre todos los sitios o sucursales de los clientes y su total aislamiento de otras VPNs. Sin embargo, los modelos de VPN en la capa IP tienen requerimientos más complejos, debido a que deben proporcionar conectividad entre diferentes VPNs e incluso proporcionar conectividad a Internet. Con la implementación de MPLS VPN es posible realizar todo tipo de escenarios e implementaciones que exijan el cumplimiento de todos los requerimientos anteriormente

48 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004.

mencionados. Las MPLS VPNs son posibles debido a que el proveedor de servicio ejecuta MPLS en la red troncal, lo cual suministra un desacoplamiento del plano de transmisión y el plano de control, tarea que es imposible realizar a través de IP.[49]

## 3.2. OBJETIVOS

- Configuración básica de una red MPLS.
- Configuración de tablas VRFs
- Configuración de MP-BGP entre routers PE
- Configuración de IGP de pequeña escala (rutas estáticas, RIP y EIGRP) entre routers CE y PE.
- Monitoreo de operaciones MPLS VPN.
- Configuración de OSPF como protocolo de enrutamiento ente routers CE y PE.
- Configuración de BGP como protocolo de enrutamiento ente routers CE y PE.
- Resolución de problemas para operaciones MPLS VPN.

## 3.3. DIAGRAMA DE TOPOLOGÍA

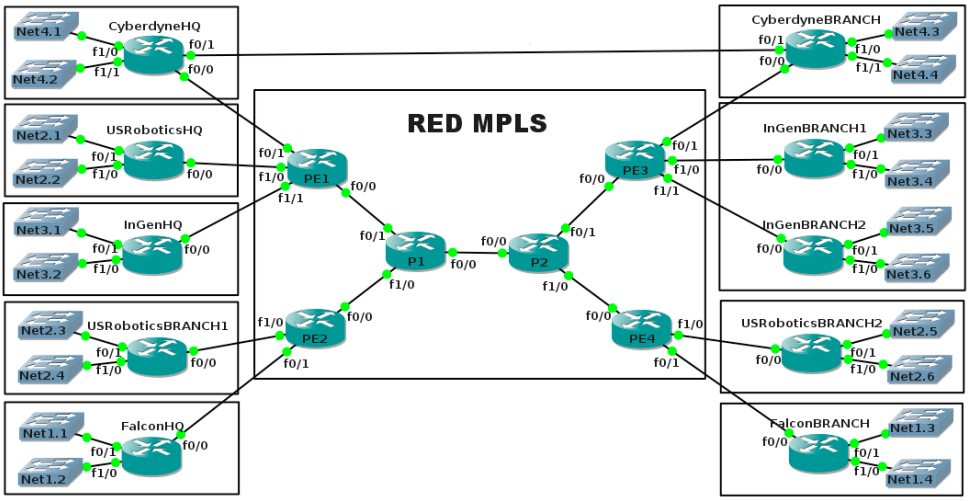


***Figura 3.1.*** Topología Implementando MPLS VPN

49 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004.

## 3.4. TABLAS DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| P1 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| | Loopback0 | | |
| P2 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| | Loopback0 | | |
| PE1 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| | FastEthernet 1/1 | | |
| | Loopback0 | | |
| PE2 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| | Loopback0 | | |
| PE3 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| | FastEthernet 1/1 | | |
| | Loopback0 | | |
| PE4 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| | Loopback0 | | |

Tabla 3.1 Implementando MPLS VPN [Red MPLS]

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| FalconHQ | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| FalconBRANCH | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |

Tabla 3.2. Implementando MPLS VPN [Cliente Falcon Air Express]

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| USRoboticsHQ | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| USRoboticsBRANCH1 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| USRoboticsBRANCH2 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |

Tabla 3.3. Implementando MPLS VPN [Cliente U.S. Robotics]

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| InGenHQ | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| InGenBRANCH1 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| InGenBRANCH2 | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |

Tabla 3.4. Implementando MPLS VPN [Cliente International Genetic Technologies, Inc]

| Dispositivo | Interfaz | Dirección IP | Máscara de Subred |
|---|---|---|---|
| CyberdHQ | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| | FastEthernet 1/1 | | |
| CyberdBRANCH | FastEthernet 0/0 | | |
| | FastEthernet 0/1 | | |
| | FastEthernet 1/0 | | |
| | FastEthernet 1/1 | | |

Tabla 3.5. Implementando MPLS VPN [Cliente Cyberdyne Systems Corporation]

## 3.5. DESCRIPCIÓN DE LA ACTIVIDAD

### TAREA 1: División en subredes del espacio de direccionamiento

**Paso 1:** Examinar los requisitos de la red

Utilice la topología que se presenta anteriormente para diseñar un esquema de direccionamiento que cumpla con los siguientes requisitos:

Para los enlaces internos de la red MPLS, se utilizará el espacio de direcciones privadas 192.168.0.0/24 para los enlaces FastEthernet que interconectan los routers P y PE, y el espacio de direcciones privadas 172.30.30.0/24 para asignar direcciones a las interfaces loopback de los routers P y PE. Divida los espacios de direcciones en subredes y registrelas en las siguientes tablas:

| Conexión | Número de subred | Subred | Máscara de Subred |
|---|---|---|---|
| P1 <> P2 | 0 | | |
| P1 <> PE1 | 1 | | |
| P1 <> PE2 | 2 | | |
| P2 <> PE3 | 3 | | |
| P2 <> PE4 | 4 | | |

El espacio de direcciones para cada cliente viene definido por el formato: 10.X.0.0/16, donde X hace referencia al número con el que se identifica el cliente de acuerdo a la siguiente tabla:

| Id. | Nombre cliente | Abreviatura | Espacio de direccionamiento |
|---|---|---|---|
| 1 | Falcon Air Express | Falcon | 10.__.0.0/16 |
| 2 | U.S. Robotics | USRob | 10.__.0.0/16 |
| 3 | International Genetic Technologies, Inc | InGen | 10.__.0.0/16 |
| 4 | Cyberdyne Systems Corporation | Cyberd | 10.__.0.0/16 |

Para el cliente Falcon Air Express, deberá asignar el espacio de direcciones para la oficina principal (FalconHQ) y para la sucursal (FalconBRANCH) cumpliendo los siguientes requisitos:

- La oficina principal necesita espacio para 16.000 hosts
- La sucursal necesita espacio para 8.000 hosts
- Los enlaces entre los sitios o sucursales y la red MPLS requieren espacio para los dos extremos de la conexión.

Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router. Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en las siguientes tablas:

| Router | Interfaz | Número de subred | Subred | Máscara Subred |
|---|---|---|---|---|
| FalconHQ | Fa1/0 | 0 | | |
| | Fa1/1 | 1 | | |

| Router | Interfaz | Número de subred | Subred | Máscara Subred |
|---|---|---|---|---|
| FalconBRANCH | Fa1/0 | 0 | | |
| | Fa1/1 | 1 | | |

| Conexión | Número de subred | Subred | Máscara de Subred |
|---|---|---|---|
| FalconHQ <> PE2 | 0 | | |
| FalconBRANCH <> PE4 | 1 | | |

Para el cliente U.S. Robotics, deberá asignar el espacio de direcciones para la oficina principal (USRobHQ) y para las sucursales (USRobBRANCH1 y USRobBRANCH2) cumpliendo los siguientes requisitos:

- La oficina principal necesita espacio para 16.000 hosts
- La primera sucursal necesita espacio para 8.000 hosts

- La segunda sucursal necesita espacio para 4.000 hosts
- Los enlaces entre los sitios o sucursales y la red MPLS requieren espacio para los dos extremos de la conexión.

Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router. Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en las siguientes tablas:

| Router | Interfaz | Número de subred | Subred | Máscara Subred |
|---|---|---|---|---|
| USRobHQ | Fa1/0 | 0 | | |
| | Fa1/1 | 1 | | |

| Router | Interfaz | Número de subred | Subred | Máscara Subred |
|---|---|---|---|---|
| USRobBRANCH1 | Fa1/0 | 0 | | |
| | Fa1/1 | 1 | | |

| Router | Interfaz | Número de subred | Subred | Máscara Subred |
|---|---|---|---|---|
| USRobBRANCH2 | Fa1/0 | 0 | | |
| | Fa1/1 | 1 | | |

| Conexión | Número de subred | Subred | Máscara de Subred |
|---|---|---|---|
| USRobHQ <> PE1 | 0 | | |
| USRobBRANCH1 <> PE2 | 1 | | |
| USRobBRANCH2 <> PE3 | 2 | | |

Para el cliente International Genetic Technologies, Inc., deberá asignar el espacio de direcciones para la oficina principal (InGenHQ) y para las sucursales (InGenBRANCH1 y InGenBRANCH2) cumpliendo los siguientes requisitos:

- La oficina principal necesita espacio para 16.000 hosts
- La sucursal necesita espacio para 8.000 hosts
- Los enlaces entre los sitios o sucursales y la red MPLS requieren espacio para los dos extremos de la conexión.

Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router. Divida el espacio de dirección para la oficina central en dos subredes iguales y el espacio de direcciones de la sucursal en cuatro subredes iguales. Registre las subredes en las siguientes tablas:

| Router | Interfaz | Número de subred | Subred | Máscara Subred |
|---|---|---|---|---|
| InGenHQ | Fa1/0 | 0 | | |
| | Fa1/1 | 1 | | |

| Router | Interfaz | Número de subred | Subred | Máscara Subred |
|---|---|---|---|---|
| InGenBRANCH1 | Fa1/0 | 0 | | |
| | Fa1/1 | 1 | | |
| InGenBRANCH2 | Fa1/0 | 2 | | |
| | Fa1/1 | 3 | | |

| Conexión | Número de subred | Subred | Máscara de Subred |
|---|---|---|---|
| InGenHQ <> PE1 | 0 | | |
| InGenBRANCH1 <> PE3 | 1 | | |
| InGenBRANCH2 <> PE3 | 2 | | |

Para el cliente Cyberdyne Systems Corporation, deberá asignar el espacio de direcciones para la oficina principal (CyberdHQ) y para la sucursal (CyberdBRANCH) cumpliendo los siguientes requisitos:

- La oficina principal necesita espacio para 16.000 hosts
- La sucursal necesita espacio para 8.000 hosts
- Los enlaces entre los sitios o sucursales y la red MPLS, y entre ellos, requieren espacio para los dos extremos de la conexión.

Comenzando por el requisito mayor, asigne un espacio de direccionamiento a cada router. Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en las siguientes tablas:

| Router | Interfaz | Número de subred | Subred | Máscara Subred |
|---|---|---|---|---|
| CyberdHQ | Fa1/0 | 0 | | |
| | Fa1/1 | 1 | | |

| Router | Interfaz | Número de subred | Subred | Máscara Subred |
|---|---|---|---|---|
| CyberdBRANCH | Fa1/0 | 0 | | |
| | Fa1/1 | 1 | | |

| Conexión | Número de subred | Subred | Máscara de Subred |
|---|---|---|---|
| CyberdHQ <> PE1 | 0 | | |
| CyberdBRANCH <> PE3 | 1 | | |
| CyberdHQ <> CyberdBRANCH | 2 | | |

**Paso 2:** Documentación del esquema de direccionamiento

Documente las direcciones que se utilizarán sobre las interfaces de los dispositivos de la red en las tablas que se presentan debajo del diagrama de la topología.

## TAREA 2: Preparación básica de la red

**Paso 1:** Conectar una red que sea similar a la del diagrama de topología

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en gráfico.

Para este laboratorio se presenta la siguiente situación: Usted está decidido en construir su propio ISP, cuenta con el capital suficiente para adquirir el equipo y las instalaciones necesarias para llevar a cabo esta ardua tarea. Se decide por empezar con una pequeña implementación de lo que implica construir una red operativa real de un ISP, y ofrecer sus servicios a unos pocos pero importantes clientes empresariales, quienes de acuerdo a las referencias sobre usted serán una gran plataforma de entrada para introducirse al enorme mercado de la prestación de servicios de comunicaciones.

Por tanto, el primer paso para lograr tan ambiciosos objetivos consiste en preparar la red MPLS para prestar servicios de comunicación a clientes, mediante la configuración de los dispositivos como se muestra a continuación.

**Paso 2:** Configuración básica de los enrutadores

Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautas generales (utilice como contraseña la palabra *"nyquist"*):

1. Configure el nombre de host del router.
2. Configure una contraseña de modo EXEC privilegiado.
3. Configure un mensaje del día.
4. Configure una contraseña para las conexiones de la consola.
5. Configure una contraseña para las conexiones de VTY.

## TAREA 3: Configurar y activar interfaces de los dispositivos

**Paso 1:** Configure las interfaces en los enrutadores con las direcciones IPde la tabla proporcionada debajo del Diagrama de topología.

## TAREA 4: Preparación previa de la red MPLS

**Paso 1:** Configurar el enrutamiento OSPF en cada uno de los routers al interior de la red MPLS

Configure todos los dispositivos con un enrutamiento OSPF al interior de la red MPLS. En la configuración asegúrese de:

- Utilizar el Id. de proceso 1 y el área 0 para las redes.

Gracias a que se utilizó explícitamente un espacio de direccionamiento privado para los enlaces internos y las interfaces Loopback, utilice el comando **network** junto con el espacio de direcciones de estas interfaces para establecer las interfaces que participaran en el enrutamiento OSPF.

**Consulte y analice:**

¿De qué rutas se encargará el IGP configurado al interior de la red MPLS?¿Por qué es importante en este caso configurar el área de OSPF con un valor de 0, teniendo en cuenta que este será el IGP que se ejecute en el núcleo de la red MPLS?

_____

_____

_____

_____

**Paso 2:** Configurar el mecanismo CEF

Habilite el mecanismo de conmutación CEF en cada uno de los routers de la red MPLS mediante el comando de configuración global **ip cef [distributed].**

**Nota:** El mecanismo de conmutación CEF se encuentra habilitado por defecto en las plataformas cisco 7100, 7200, 7500, 6500 y 12000.

## TAREA 5: Configuración de MPLS

**Paso 1:** Configurar MPLS en las interfaces participantes

En cada uno de los routers de la topología, habilite la conmutación de etiquetas en las interfaces adecuadas. Para llevar a cabo esta tarea utilice los comandos de configuración de interfaz **mpls ip** y**mpls label protocol [tdp] [ldp] [both].**
**Paso 2:** Configurar el MPLS ID

Especifique el MPLS ID de cada uno de los routers al interior de la red MPLS mediante el comando en el modo de configuración global:

**mpls ldp** <*router-id*> **interface** [**force**]

Asegúrese que cada router en la red MPLS utilice la dirección de su interface Loopback 0 como identificador.

**Paso 3:** Configurar autenticación para MPLS

Configure la autenticación en cada uno de los routers de la red MPLS mediante el comando en modo de configuración global:
**mpls ldp neighbor** <*neighbor-ip-address*> **password** <*password*>

Asegúrese que cada router en la red MPLS este configurado con la contraseña "nyquist" para cada uno de sus vecinos, porque de lo contrario no se establecerán las adyacencias.

## TAREA 6: Asegúrese que se establecieron las configuraciones de forma correcta

- Asegúrese de haber establecido de forma correcta la configuración MPLS en las interfaces adecuadas de cada uno de los routers cisco de la red mediante el comando: show mpls interfaces [<interface>][detail].

- Supervise el estado del proceso de descubrimiento LDP mediante el comando: show mpls ldp discovery.

- Asegúrese de haber generado las adyacencias de forma correcta mediante el comando:
- show mpls ldp neighbor [vrf <vrf-name>] [address][interface][detail][all]

- Asegúrese que el contenido de la tabla LIB para cada uno los routers cisco sea el correcto. Utilice el commando:
- show mpls ldp bindings [vrf <vrf-name>] [network {mask|length} [longer-prefixes]][local-label <label>[<label>]] [remote-label <label> [<label>]] [neighbor <ip-address>] [local]

- Asegúrese que el contenido de la tabla LFIB para cada uno los routers cisco sea el correcto. Utilice el commando:
- show mpls forwarding-table [network {mask|length}| labels <label>[- <label>] | interface interface | next-hop <address>| lsp-tunnel [<tunnel-id>]] [detail]
- Asegúrese que el contenido de la tabla FIB para cada uno los routers cisco sea el correcto. Utilice el comando:
- show ip cef [unresolved | summary]

## TAREA 7: Configurar MP-BGP entre los routers PE

**Consulte y analice:** Defina los siguientes conceptos en pocas palabras:

**VC:**

_____
_____
_____

**PVC:**

_____
_____
_____

**SVC:**

_____
_____
_____

**VPN:**

_____
_____
_____

**P-Network:**

_____
_____
_____

**C-Network:**

_____
_____
_____

**Router P:**

_____
_____
_____

**Router PE:**

_____
_____
_____

**POP:**

_____
_____
_____

**Router CE:**

_____
_____
_____

**Sitio o sucursal:**

_____
_____
_____

Anteriormente, para proveer servicios de VPNs a sus clientes, los ISPs debían escoger entre dos modelos diferentes: **Overlay VPN** o **Peer-to-Peer VPN**.[50]

El modelo **Overlay VPN** consiste en la creación de circuitos virtuales permanentes (PVCs) entre los diferentes sitios o sucursales de un cliente[51]. Entre los beneficios que trae este modelo se encuentra:[52]

- La facilidad de implementación, tanto en la perspectiva del cliente como en la del proveedor.
- El proveedor de servicio no tiene que participar en el enrutamiento del cliente, por lo tanto, las responsabilidades del proveedor de servicio y las del cliente se encuentran bien definidas, haciendo que el punto de demarcación sea de fácil administración.

Sin embargo este modelo trae desventajas como:[53]

- Se hace necesaria una malla completa entre los sitios del cliente para proveer enrutamiento óptimo entre ellos.
- Todos los circuitos virtuales entre los sitios de los clientes deben ser configurados manualmente, y el ancho de banda debe ser asignado sobre una base sitio a sitio, requerimiento que puede llegar a ser difícil de satisfacer.
- Las implementaciones de Overlay VPN basadas en IP (IPSec o GRE) incurren en altos costos por encapsulamiento.

50 GHEIN, Luc De. MPLS Fundamentals. Cisco Press. Estados Unidos. 2007. p. 10.

51 Ibíd., p. 10.

52 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 308.

53 Ibíd., p. 309.

El modelo **Peer-to-Peer VPN** fue introducido para dar solución a los inconvenientes causados por el modelo Overlay VPN, y proveer un óptimo transporte de información a través del backbone del proveedor de servicio. En este modelo, el proveedor de servicio participa activamente en el enrutamiento del cliente, aceptando rutas, transportándolas a través de su propio backbone, y finalmente propagándolas a otros sitios del cliente.[54]

La implementación más común del modelo Peer-to-Peer VPN consiste en la utilización de filtros de paquetes sobre los routers PE de un proveedor para aislar clientes, quienes pueden compartir el mismo router PE. En esta implementación era común para el proveedor de servicio asignar una porción de su propio espacio de direcciones a cada cliente y administrar filtros de paquetes en los routers PE para asegurar una completa accesibilidad entre los sitios de un sólo cliente y el aislamiento entre clientes diferentes.[55]

El mantenimiento de filtros de paquetes es una tarea tediosa y propensa a errores, por lo tanto, algunos proveedores de servicio implementaron soluciones más innovadoras basadas en distribución controlada de rutas. En esta propuesta, el cliente estaba conectado a un router PE dedicado, el cual contenía sólo las rutas de ese único cliente, mientras que los routers P en el núcleo de la red contenían todas las rutas de los clientes. Esta implementación requiere un router PE dedicado por cliente por punto de presencia (POP). El aislamiento del cliente es logrado solamente gracias a la falta de información de enrutamiento en el router PE.[56]

Aunque el modelo Peer-to-Peer VPN solucionaba muchos de los problemas del modelo Overlay VPN, este también traía consigo otra clase de inconvenientes:[57]

- El proveedor de servicio se vuelve responsable del correcto enrutamiento del cliente y de la rápida convergencia de la red del cliente después de una caída del enlace.
- Los routers PE tienen que manejar todas las rutas de los clientes que estaban ocultas para el proveedor de servicio en el modelo Overlay VPN.
- El proveedor de servicio necesita conocimiento detallado del enrutamiento IP, lo cual no se encuentra fácilmente en los equipos de trabajo del proveedor de servicio tradicional.

La arquitectura **MPLS VPN** fue introducida para ofrecer a los proveedores de servicio una arquitectura Peer-to-Peer VPN que combina las mejores características de las Overlay VPNs (soporte para el sobrelapamiento de espacios de direcciones de clientes) con las mejores características de las Peer-to-Peer VPNs, como se describe a continuación:[58]
v

54 GHEIN, Luc De. MPLS Fundamentals. Cisco Press. Estados Unidos. 2007. p. 12

55 Ibíd, p. 12.

56 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 307.

57 Ibíd., p. 309.

58 Ibíd., p. 328.

- Los routers PE participan en el enrutamiento de los clientes, garantizando enrutamiento óptimo entre los sitios o sucursales de los clientes.
- Los routers PE manejan un conjunto separado de rutas para cada cliente, ofreciendo un aislamiento completo entre los clientes.
- Los clientes pueden utilizar direcciones sobrelapadas.

La arquitectura de un router PE en una MPLS VPN consiste en múltiples instancias de tablas de enrutamiento virtuales asignadas a cada cliente, las cuales se encuentran condensadas sobre un mismo dispositivo físico, simulando ser routers PE dedicados como los presentes en el modelo Peer-to-Peer VPN tradicional. El enrutamiento a través del backbone del proveedor es realizado por un proceso de enrutamiento independiente que utiliza una tabla de enrutamiento IP global.[59]

Aunque las tablas de enrutamiento virtuales proveen aislamiento entre los vecinos, sigue siendo necesario que la información que se encuentra en estas tablas sea intercambiada entre los routers PE para habilitar la transferencia de información entre sitios o sucursales del cliente conectados a diferentes routers PE. Por lo tanto, es necesario implementar un protocolo de enrutamiento que pueda transportar todas las rutas de los clientes a través de la red P, mientras mantiene la independencia entre los espacios de direcciones de clientes individuales.[60]

La mejor solución para el problema de propagación de rutas del cliente es implementar un único protocolo de enrutamiento que se ejecute únicamente entre los routers PE, liberando a los routers P de la carga de participar en las decisiones de enrutamiento de los clientes. Debido a que se espera que el número total de rutas de los clientes sea muy grande, el único protocolo de enrutamiento dinámico que cumple con el requerimiento de escalabilidad es BGP. Por lo tanto, BGP se utiliza en la arquitectura MPLS VPN para el transporte de las rutas de los clientes directamente entre routers PE.[61]

Sin embargo, la implementación de un único protocolo de enrutamiento conlleva a un dilema sobre la forma de transportar múltiples prefijos de ruta idénticos de diferentes clientes entre los routers PE. La solución para este inconveniente consiste en la expansión de los prefijos IP de los cliente mediante un identificador único convirtiéndolos en prefijos únicos inclusive si anteriormente se sobrelapaban. Un prefijo de 64 bits llamado el RD se utiliza en las MPLS VPNs para convertir las direcciones IPv4 de 32 bits de los clientes que pueden sobrelaparse entre ellas, en direcciones VPNv4 únicas de 96 bits que pueden ser transportadas entre los routers PE. Una sesión entre routers PE es llamada sesión BGP Multiprotocolo (MP-BGP).[62]

59 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p., p. 330.

60 Ibíd., p. 331.

61 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p. 334.

62 ARIGANELLO, Ernesto; BARRIENTOS, Ernesto. REDES CISCO. CCNP a fondo. Guía de estudio para profesionales. Primera Edición. Alfaomega Grupo Editor. México. 2010. p. 599.

La única función del RD (Router Distinguisher) es la de convertir las direcciones IPv4, en direcciones únicas globalmente, sin embargo no puede indicar que un sitio participa en más de una VPN[63]. Los RTs (Route Targets) son atributos que se adjuntan a una ruta BGP VPNv4 para indicar su membresía a una VPN. Las extended BGP communities de las actualizaciones de enrutamiento son utilizadas para transportar el RT y así identificar a cual VPN pertenece cada actualización en particular.[64]

**Paso 1:** Establecer mallas completas de sesiones IBGP entre las interfaces de los routers PE al interior de la red MPLS

Establezca mallas completas de sesiones IBGP únicamente entre los routers PE al interior de la red MPLS, recuerde que los routers P no deben participar en las sesiones IBGP con el objetivo de liberarlos de la carga de participar en el enrutamiento del cliente.

**Paso 2:** Configurar el intercambio de rutas VPNv4 para habilitar el enrutamiento MP-BGP

Habilite el intercambio de rutas VPNv4 entre los routers PE mediante el siguiente comando:

**router(config-router)#address-family vpnv4**

Para especificar los vecinos que participarán en el intercambio de rutas VPNv4, haga uso del siguiente comando:

**router(config-router-af)#neighbor** <*neighbor-ip-address*> **activate**

Y especifique al router PE como el próximo salto para evitar inconvenientes si tiene sesiones EBGP contiguas con un vecino CE, utilice el siguiente comando para llevar a cabo esta tarea:

**router(config-router-af)#neighbor** <*neighbor-ip-address*> **next-hop-self**

Posteriormente se debe habilitar la propagación de las extended BGP communities, utilizando el siguiente comando:
**neighbor** <*neighbor-ip-address*> **send-community** [**extended** | **both**]

## TAREA 8: Prestación de servicios para el cliente Falcon Air Express

Una vez que la red MPLS se encuentre operativa, ya es posible prestar el servicio de conectividad a clientes. El primer cliente, es la aerolínea de carga Falcon Air Express, quien ha contratado sus servicios para comunicar su oficina principal con las oficinas ubicadas en la sucursal remota.

**Paso 1:** Configurar RIP sobre los routers CE

63 Ibíd., p. 599.

64 Ibíd., p. 600.

Inicialmente, se debe configurar el protocolo de enrutamiento dinámico RIP sobre los routers CE, para lo cual no se deben incluir comandos adicionales.

**Paso 2:** Configurar VRFcliente Falcon Air Express

Configurar una nueva VRF para el cliente por medio del comando:

**ip vrf**<*vrf-name*>
**rd**<*rd-value*>
**route-target** {**import** | **export** |**both**} <*rt-value*>

Para los atributos rd-value y rt-value se utilizan los formatos asn:nn o a.b.c.d:nn, en este caso se utilizará el primero de ellos teniendo en cuenta las siguientes especificaciones:

- asn: Número AS del Proveedor de Servicio (AS 123)
- nn: Número con el formato X00, donde X es el número de identificación del cliente.

**Paso 3:** Asociar interfaces de los router PE a la VRF

Definir las interfaces sobre los routers PE que se conectaran directamente a los router CE del cliente, asociándolas a la VRF anteriormente definida. Esta actividad se realiza mediante el uso del comando:

**ip vrf forwarding** <*vrf-name*>

**Nota:** El anterior comando debe ser utilizado antes de configurar el direccionamiento IP sobre las interfaces, debido a que el uso del mismo elimina las direcciones IP asignadas a una interfaz.

**Paso 4:** Configurar RIP sobre los routers PE

Debido a que el cliente está ejecutando RIP como el IGP para su red interna, es necesario configurar el enrutamiento RIP sobre los routers PE directamente conectados. Sólo la versión 2 de RIP es soportado como protocolo de enrutamiento entre routers PE y CE.
**Paso 5:** Configurar contexto de enrutamiento para RIP

Configurar el contexto de enrutamiento individual de RIP para la VRF anteriormente definida del cliente Falcon Air Express, sobre los routers PE directamente conectados a los equipos CPE de las sucursales remotas. Para llevar a cabo esta tarea, utilice el siguiente comando en modo de configuración de router:

**address-family ipv4 vrf**<*vrf-name*>

Habilite en el contexto de enrutamiento RIP las interfaces de los routers PE que participan en el intercambio de actualizaciones RIP con los respectivos routers CE del cliente.

Configure la redistribución de rutas de RIP sobre BGP, con el objetivo de transportar sobre la red MPLS las rutas aprendidas dinámicamente a través del IGP. Para llevar a cabo esta tarea, utilice el siguiente comando en el modo de configuración de contexto de enrutamiento de la VRF del cliente:

**redistribute bgp**<*as-number*>**metric transparent**

**Consulte y analice:**

¿Qué función cumple el uso de la opción **metric transparent** en el comando de redistribución de rutas?

_____

_____

_____

_____

**Paso 6:** Establecer conectividad RIP de extremo a extremo

Se debe configurar un contexto de enrutamiento de BGP para cada VRF, a través del comando en el modo de configuración de router:

**address-family ipv4 vrf**<*vrf-name*>

Posteriormente, se deben redistribuir las rutas RIP sobre BGP para cada VRF sobre la cual se haya configurado el contexto de enrutamiento de RIP, para llevar a cabo esta tarea se debe hacer uso del siguiente comando en modo de configuración de contexto de enrutamiento:

**redistribute rip**

**Paso 7:** Verificar las conexiones y la conectividad
Verificar la información correspondiente a los protocolos de enrutamiento por VRF en el router PE con el comando:

**show ip protocols vrf**<*vrf-name*>

Verificar la tabla de enrutamiento por VRF en el router PE con el comando:

**show ip route vrf**<*vrf-name*>

Para visualizar la tabla de enrutamiento BGP asociada con el VRF del cliente, utilice el comando:

**show ip bgp vpnv4 vrf**<*vrf-name*>

Sobre los equipos CPE del cliente, verificar que se estén aprendiendo todas las rutas dinámicas anunciadas desde las sedes remotas a través del comando:

**show ip route**

Para verificar la conectividad a través de la VPN, realizar pruebas de ping y traceroute desde los equipos CPE del cliente, a través de los comandos:

**ping**<*ip_address*>**source**{<*source_address*> | <*source_interface*>}

**trace**<*ip_address*>**source**{<*source_address*> | <*source_interface*>}

Realice pruebas de ping y traceroute desde los equipos PE, a través de los comandos:

**pingvrf**<*vrf_name*><*ip_address*>**source**{<*source_address*> | <*source_interface*>}

**tracevrf**<*vrf_name*><*ip_address*>**source**{<*source*_address> | <*source_interface*>}

## TAREA 9: Prestación de servicios para el cliente U.S. Robotics

**Paso 1:** Configurar EIGRP sobre los routers CE

Inicialmente, se debe configurar el protocolo de enrutamiento dinámico EIGRP sobre los routers CE, para lo cual no se deben incluir comandos adicionales.

**Paso 2:** Configurar VRFcliente U.S. Robotics

Configurar una nueva VRF para el cliente por medio del comando:

**ip vrf**<*vrf-name*>
**rd**<*rd-value*>
**route-target** {**import** | **export** |**both**} <*rt-value*>

Para los atributos rd-value y rt-value se utilizan los formatos asn:nn o a.b.c.d:nn, en este caso se utilizará el primero de ellos teniendo en cuenta las siguientes especificaciones:
asn: Número AS del Proveedor de Servicio (AS 123)
nn: Número con el formato X00, donde X es el número de identificación del cliente.

**Paso 3:** Asociar interfaces de los router PE a la VRF

Definir las interfaces sobre los routers PE que se conectaran directamente a los router CE del cliente, asociándolas a la VRF anteriormente definida. Esta actividad se realiza mediante el uso del comando:

**ip vrf forwarding** <*vrf-name*>

**Nota:** El anterior comando debe ser utilizado antes de configurar el direccionamiento IP sobre las interfaces, debido a que el uso del mismo elimina las direcciones IP asignadas a una interfaz.

**Paso 4:** Configurar EIGRPsobre los routers PE

Debido a que el cliente está ejecutando EIGRP como el IGP para su red interna, es necesario configurar el proceso global de EIGRP sobre los routers PE asignados para el cliente Genetic Technologies, Inc. Utilice 1 como ID de proceso

**Paso 5:**Configurar el contexto de enrutamiento EIGRP

Configurar el contexto de enrutamiento sobre el proceso global de EIGRP para la instancia VRF definida anteriormente para el cliente U.S. Robotics, especificando como número de Sistema Autónomo el número del proceso de enrutamiento EIGRP configurado sobre los routers CPE ubicados en las sedes remotas del cliente. Para llevar a cabo esta tarea utilice el comando:

**address-family ipv4 vrf**<*vrf-name*>**autonomous-system**<*as-number*>

Habilite en el contexto de enrutamiento EIGRP las interfaces de los routers PE que participan en el intercambio de actualizaciones EIGRP con los respectivos routers CE del cliente. Para llevar a cabo esta tarea haga uso del comando **network**.

Configure la redistribución desde BGP sobre EIGRP de las rutas relacionadas con la instancia VRF relacionada con el cliente U.S. Robotics, mediante el comando:
**redistribute bgp** <*as-number*>**metric** <*metric-value*>

**Paso 6:** Establecer conectividad EIGRP de extremo a extremo

Configurar un contexto de enrutamiento del proceso global BGP, asociándolo con la tabla VRF del cliente U.S. Robotics.

**address-family ipv4 vrf**<*vrf-name*>

Redistribuya las rutas EIGRP vinculadas a este cliente haciendo referencia al número de proceso EIGRP configurado sobre los routers CPE ubicados en las sedes remotas del cliente. Lleve a cabo esta operación a través del comando:

**redistribute eigrp** <*process-id*>

**Paso 7:** Verificar las conexiones y la conectividad

Verificar la información correspondiente a los protocolos de enrutamiento por VRF en el router PE con el comando:

**show ip protocols vrf**<*vrf-name*>

Verificar la tabla de enrutamiento por VRF en el router PE con el comando:

**show ip route vrf**<*vrf-name*>

Para visualizar la tabla de enrutamiento BGP asociada con el VRF del cliente, utilice el comando:

**show ip bgp vpnv4 vrf**<*vrf-name*>

Sobre los equipos CPE del cliente, verificar que se estén aprendiendo todas las rutas dinámicas anunciadas desde las sedes remotas a través del comando:

**show ip route**

Para verificar la conectividad a través de la VPN, realizar pruebas de ping y traceroute desde los equipos CPE del cliente, a través de los comandos:

**ping**<*ip_address*>**source**{<*source_address*> | <*source_interface*>}

**trace**<*ip_address*>**source**{<*source_address*> | <*source_interface*>}

Realice pruebas de ping y traceroute desde los equipos PE, a través de los comandos:

**pingvrf**<*vrf_name*><*ip_address*>**source**{<*source_address*> | <*source_interface*>}

**tracevrf**<*vrf_name*><*ip_address*>**source**{<*source*_address> | <*source_interface*>}

## TAREA 10: Prestación de servicios para el cliente International Genetic Technologies, Inc

**Paso 1:** Configurar OSPF sobre los routers CE

Inicialmente, se debe configurar el protocolo de enrutamiento dinámico EIGRP sobre los routers CE, para lo cual no se deben incluir comandos adicionales.

**Paso 2:** Configurar VRFcliente International Genetic Technologies, Inc.

Configurar una nueva VRF para el cliente por medio del comando:

**ip vrf**<*vrf-name*>
**rd**<*rd-value*>
**route-target** {**import | export |both**} <*rt-value*>

Para los atributos rd-value y rt-value se utilizan los formatos asn:nn o a.b.c.d:nn, en este caso se utilizará el primero de ellos teniendo en cuenta las siguientes especificaciones:

- asn: Número AS del Proveedor de Servicio (AS 123)
- nn: Número con el formato X00, donde X es el número de identificación del cliente.

**Paso 3:** Asociar interfaces de los router PE a la VRF

Definir las interfaces sobre los routers PE que se conectaran directamente a los router CE del cliente, asociándolas a la VRF anteriormente definida. Esta actividad se realiza mediante el uso del comando:

**ip vrf forwarding** <*vrf-name*>

**Nota:** El anterior comando debe ser utilizado antes de configurar el direccionamiento IP sobre las interfaces, debido a que el uso del mismo elimina las direcciones IP asignadas a una interfaz.

**Paso 4:** Configurar OSPF sobre los routers PE

Debido a que el cliente está ejecutando OSPF como el IGP para su red interna, es necesario configurar el proceso de enrutamiento de OSPF sobre los routers PE asignados para el cliente International Genetic Technologies, Inc.

Se debe asociar el proceso de OSPF para la instancia VRF definida anteriormente para el cliente International Genetic Technologies, Inc., para llevar a cabo esta tarea utilice el comando:

**router ospf** <*process-id*>**vrf** <*vrf-name*>

Habilite en el proceso de enrutamiento OSPF las interfaces de los routers PE que participan en el intercambio de actualizaciones OSPF con los respectivos routers CE del cliente. Para llevar a cabo esta tarea haga uso del comando **network**.

Configure la redistribución desde BGP sobre OSPF de las rutas relacionadas con la instancia VRF relacionada con el cliente International Genetic Technologies, Inc., mediante el comando:

**redistribute bgp** <*as-number*>**subnets**

**Paso 5:** Establecer conectividad EIGRP de extremo a extremo

Configurar un contexto de enrutamiento del proceso global BGP, asociándolo con la tabla VRF del cliente International Genetic Technologies, Inc.

**address-family ipv4 vrf**<*vrf-name*>

Redistribuya las rutas OSPF vinculadas a este cliente haciendo referencia al número de proceso OSPF configurado sobre los routers CPE ubicados en las sedes remotas del cliente. Lleve a cabo esta operación a través del comando:

**redistribute ospf**<*process-id*>[**match** [**internal**] [**external 1**] [**external 2**]]

**Nota:** Si no se especifica la palabra clave **match**, sólo las rutas OSPF internal son redistribuidas.

**Paso 6:** Verificar las conexiones y la conectividad

Verificar la información correspondiente a los protocolos de enrutamiento por VRF en el router PE con el comando:

**show ip protocols vrf**<*vrf-name*>

Verificar la tabla de enrutamiento por VRF en el router PE con el comando:
**show ip route vrf**<*vrf-name*>

Para visualizar la tabla de enrutamiento BGP asociada con el VRF del cliente, utilice el comando:

**show ip bgp vpnv4 vrf**<*vrf-name*>

Sobre los equipos CPE del cliente, verificar que se estén aprendiendo todas las rutas dinámicas anunciadas desde las sedes remotas a través del comando:

**show ip route**

Para verificar la conectividad a través de la VPN, realizar pruebas de ping y traceroute desde los equipos CPE del cliente, a través de los comandos:

**ping**<*ip_address*>**source**{<*source_address*> | <*source_interface*>}

**trace**<*ip_address*>**source**{<*source_address*> | <*source_interface*>}

Realice pruebas de ping y traceroute desde los equipos PE, a través de los comandos:

**pingvrf**<*vrf_name*><*ip_address*>**source**{<*source_address*> | <*source_interface*>}

**tracevrf**<*vrf_name*><*ip_address*>**source**{<*source*_address> | <*source_interface*>}

## TAREA 11: Prestación de servicios para el cliente Cyberdyne Systems Corporation

**Paso 1:** Configurar BGP sobre los routers CE

Inicialmente, se debe configurar el protocolo de enrutamiento dinámico BGP sobre los routers CE, para lo cual no se deben incluir comandos adicionales. Para llevar a cabo esta configuración, se asignó el número de AS 4000 para el cliente.

Configure las vecindades entre los router CE y anuncie las redes LAN que se encuentran detrás de los equipos CPE ubicados en las sucursales del cliente, para llevar a cabo esta tarea utilice el comando**network.**

**Paso 2:** Configurar VRF cliente Cyberdyne Systems Corporation

Configurar una nueva VRF para el cliente por medio del comando:

**ip vrf** <*vrf-name*>
  **rd** <*rd-value*>
  **route-target** {**import** | **export** | **both**} <*rt-value*>

Para los atributos rd-value y rt-value se utilizan los formatos asn:nn o a.b.c.d:nn, en este caso se utilizará el primero de ellos teniendo en cuenta las siguientes especificaciones:

- asn: Número AS del Proveedor de Servicio (AS 123)
- nn: Número con el formato X00, donde X es el número de identificación del cliente.

**Paso 3:** Asociar interfaces de los router PE a la VRF

Definir las interfaces sobre los routers PE que se conectaran directamente a los router CE del cliente, asociándolas a la VRF anteriormente definida. Esta actividad se realiza mediante el uso del comando:

**ip vrf forwarding** <*vrf-name*>

**Nota:** El anterior comando debe ser utilizado antes de configurar el direccionamiento IP sobre las interfaces, debido a que el uso del mismo elimina las direcciones IP asignadas a una interfaz.

**Paso 4:** Configurar contexto de enrutamiento BGP sobre los routers PE

Debido a que el cliente está ejecutando BGP como el IGP para su red interna, es necesario configurar el contexto de enrutamiento de BGP sobre los routers PE asignados para el cliente Cyberdyne Systems Corporation.

Se debe asociar el contexto de enrutamiento de BGP para la instancia VRF definida anteriormente para el cliente Cyberdyne Systems Corporation, para llevar a cabo esta tarea utilice el comando en el modo de configuración de router:

**address-family ipv4 vrf** <*vrf-name*>

Establezca vecindades entre los routers CE y PE, para estos últimos se deben definir las sesiones con los pares BGP sobre el contexto de enrutamiento BGP, para llevar a cabo esta tarea haga uso del comando:

**neighbor** <*neighbor-ip-address*>**remote-as** <*as-number*>

Por último se utiliza el mecanismo**as-override**, el cual modifica el atributo AS-path de una actualización de ruta BGP, sobreescribiendo el número AS propio del cliente por el número AS del ISP una vez que la actualización cruza las fronteras de la red MPLS.

**neighbor** <*neighbor-ip-address*>**as-override**

**Consulte y analice:**

¿Por qué se hace necesario utilizar el mecanismo **as-override** cuando se utiliza BGP como protocolo de enrutamiento interno en redes remotas que pertenecen a un mismo AS?

_____

_____

_____

_____

**Paso 5:** Seleccionar el enlace primario y el secundario con BGP

Entre las sucursales remotas del cliente  Cyberdyne Systems Corporation, se ha contratado un enlace dedicado que conecta directamente las redes de ambas sedes. Este enlace provee

un bajo ancho de banda el cual ha sido insuficiente para el tráfico intercambiado entre estas sucursales.

El cliente ha contratado un enlace con un mayor ancho de banda a través de la red MPLS, el cual utilizará como enlace primario para el tráfico generado desde las redes de las sucursales. Adicionalmente, ha decidido dejar el enlace anterior como enlace de respaldo.

Teniendo en cuenta los requerimientos definidos por el cliente, realice las configuraciones pertinentes sobre BGP para lograr el resultado esperado.

**Paso 6:** Verificar las conexiones y la conectividad

Verificar la información correspondiente a los protocolos de enrutamiento por VRF en el router PE con el comando:

**show ip protocols vrf**<*vrf-name*>

Verificar la tabla de enrutamiento por VRF en el router PE con el comando:

**show ip route vrf**<*vrf-name*>

Para visualizar la tabla de enrutamiento BGP asociada con el VRF del cliente, utilice el comando:
**show ip bgp vpnv4 vrf**<*vrf-name*>

Sobre los equipos CPE del cliente, verificar que se estén aprendiendo todas las rutas dinámicas anunciadas desde las sedes remotas a través del comando:

**show ip route**

Para verificar la conectividad a través de la VPN, realizar pruebas de ping y traceroute desde los equipos CPE del cliente, a través de los comandos:

**ping**<*ip_address*>**source**{<*source_address*> | <*source_interface*>}

**trace**<*ip_address*>**source**{<*source_address*> | <*source_interface*>}

Realice pruebas de ping y traceroute desde los equipos PE, a través de los comandos:

**pingvrf**<*vrf_name*><*ip_address*>**source**{<*source_address*> | <*source_interface*>}

**tracevrf**<*vrf_name*><*ip_address*>**source**{<*source*_address> | <*source_interface*>}

# 4. LABORATORIO NO. 4 -MPLS VPNSs COMPLEJAS

## 4.1. INTRODUCCION

Para indicar que un sitio pertenece a muchas MPLS VPN hace falta un método adecuado en el que un conjunto de identificadores VPN pueda ser unido a unas rutas para indicar esa asociación. Un RD es el método apropiado para una simple VPN; los RTs se crearon para participar en topologías VPN más complejas.

Un RT es un atributo adicional que es aplicado a un prefijo IPv4 de BGP para indicar asociación a una VPN. El RT es asociado a la ruta una vez que es convertida a ruta VPNv4 por los routers PE. Los RTs adjuntos a la ruta son llamados *export RT* e identifican las VPNs a las cuales los sitios asociados en particular con una VRF pertenecen. Los adjuntos a las VRFs se denominan *import RT* e identifican las rutas asociadas con una VRF en particular. Cada VRF en un router PE pueden tener múltiples *import RT* que identifican el conjunto de VPNs desde las cuales esta VRF está aceptando rutas.

Este laboratorio está orientado comprender de forma precisa los atributos RT y como a través de estos se pueden generar topologías VPN más complejas.

## 4.2. OBJETIVOS

- Funciones avanzadas de importación y exportación VRF.
- Características principales de la solución Overlapping VPN.
- Implementación de la solución Overlapping VPN mediante la configuración de las características avanzadas RT.
- Descripción general la solución Central Services VPN.
- Implementación de la solución Central Services VPN a través de las características avanzadas import-export RT.
- Características principales de la solución Managed CE routersService.
- Implementación de la solución Managed CE routersService.

## 4.3. DIAGRAMA DE TOPOLOGIA

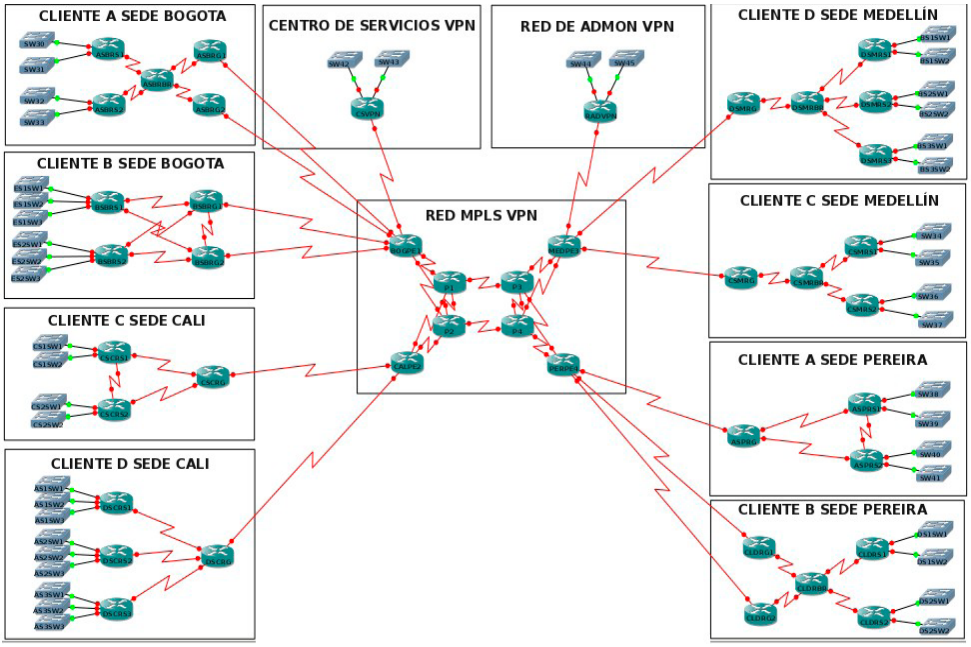


***Figura 4.1.*** Topología MPLS VPNs complejas

## 4.4. TABLAS DE DIRECCIONAMIENTO

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| BOG-PE1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Serial1/4 | | |
| | Serial1/5 | | |
| | Serial1/6 | | |
| | Loopback0 | | |
| CAL-PE2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback0 | | |
| MED-PE3 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Serial1/4 | | |
| | Loopback0 | | |
| PER-PE4 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Serial1/4 | | |
| | Loopback0 | | |
| P1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| P2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback0 | | |
| P3 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback0 | | |
| P4 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback0 | | |

Tabla 4.1. MPLS VPNs complejas [Dominio MPLS VPN]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CS-VPN | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 4.2. MPLS VPNs complejas [Centro de Servicios VPN]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| RAD-VPN | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 4.3. MPLS VPNs complejas [Red de Admon VPN]

| **Dispositivo** | **Interfaz** | **Dirección IP** | **Máscara de subred** |
|---|---|---|---|
| ASB-RG1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Loopback0 | | |
| ASB-RG2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Loopback0 | | |
| ASB-RBR | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| ASB-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| ASB-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 4.4. MPLS VPNs complejas [Cliente A sede Bogotá]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| ASP-RG | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Loopback0 | | |
| ASP-RS1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| ASP-RS2 | Serial1/0 | | |
| | Serial1/1 | | |

| | | | |
|---|---|---|---|
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 4.5. MPLS VPNs complejas [Cliente A sede Pereira]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| BSP-RG1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Loopback0 | | |
| BSP-RG2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Loopback0 | | |
| BSP-RBR | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| BSP-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| BSP-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 4.6. MPLS VPNs complejas [Cliente B sede Pereira]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| BSB-RG1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback0 | | |
| BSB-RG2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| BSB-RS1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |
| BSB-RS2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |

Tabla 4.7. MPLS VPNs complejas [Cliente B sede Bogotá]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CSC-RG | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Loopback0 | | |
| CSC-RS1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| CSC-RS2 | Serial1/0 | | |
| | Serial1/1 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 4.8. MPLS VPNs complejas [Cliente C sede Cali]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| CSM-RG | Serial1/0 | | |
| | Serial1/1 | | |
| | Loopback0 | | |

| | | | |
|---|---|---|---|
| CSM-RBR | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| CSM-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| CSM-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 4.9. MPLS VPNs complejas [Cliente C sede Medellín]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| DSC-RG | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| | Loopback0 | | |
| DSC-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |
| DSC-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |
| DSC-RS3 | Serial1/0 | | |
| | Ethernet2/0 | | |

| | | | |
|---|---|---|---|
| | Ethernet2/1 | | |
| | Ethernet2/2 | | |

Tabla 4.10. MPLS VPNs complejas [Cliente D sede Cali]

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|

| | | | |
|---|---|---|---|
| DSM-RG1 | Serial1/0 | | |
| | Serial1/1 | | |
| | Loopback0 | | |
| DSM-RBR | Serial1/0 | | |
| | Serial1/1 | | |
| | Serial1/2 | | |
| | Serial1/3 | | |
| DSM-RS1 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| DSM-RS2 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |
| DSM-RS3 | Serial1/0 | | |
| | Ethernet2/0 | | |
| | Ethernet2/1 | | |

Tabla 4.11. MPLS VPNs complejas [Cliente D sede Medellín]

# 4.5. DESCRIPCIÓN DE LA ACTIVIDAD

**TAREA 1: Diseñar y documentar un esquema de direccionamiento**
**Paso 1:** Diseñe un esquema de direccionamiento.
Utilice la topología mostrada previamente y diseñe el esquema de direccionamiento con base en los requisitos que plantea cada cliente al igual que los requisitos planteados por la red MPLS VPN.

**Nota:** Para cada cliente deberá asignar a cada router de sucursal un espacio de dirección según los requisitos planteados empezando por el requisito. Para todas las direcciones de subred de Loopback utilice la subred 10.15.15.0/25.

## Cliente A sede Bogotá

El espacio de direccionamiento para la red del cliente Asede Bogotá es el bloque de direcciones 10.1.0.0/20.

- ASB-RS1 necesita espacio para 2000 hosts _____
- ASB-RS2 necesita espacio para 1000 hosts

Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| ASB-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| ASB-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

Para las WAN en la red del cliente A sede Bogotá realice las conexiones con la dirección 170.16.0.0/27. Registre las subredes en la siguiente tabla:

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| ASB-RS1 <>ASB-RBR | 0 | | |
| ASB-RS2 <>ASB-RBR | 1 | | |
| ASB-RG1 <>ASB-RBR | 2 | | |
| ASB-RG2 <>ASB-RBR | 3 | | |

## Cliente A sede Pereira

El espacio de direccionamiento para la red del cliente A sede Pereira es el bloque de direcciones 10.2.0.0/19.

- ASP-RS1 necesita espacio para 4000 hosts
- ASP-RS2 necesita espacio para 2000 hosts

Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| ASP-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| ASP-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

Para las WAN en la red del cliente A sede Pereira, realice las conexiones con la dirección 170.17.0.0/28. Registre las subredes en la siguiente tabla:

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| ASP-RS1 <>ASP-RG | 0 | | |
| ASP-RS2 <>ASP-RG | 1 | | |
| ASP-RS1 <>ASP-RS2 | 2 | | |

## Cliente B sede Pereira

El espacio de direccionamiento para la red del cliente B sede Pereira es el bloque de direcciones 11.1.0.0/20.

- BSP-RS1 necesita espacio para 2000 hosts
- BSP-RS2 necesita espacio para 1000 hosts

Divida el espacio de direccionamiento para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| BSP-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| BSP-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

Para las WAN en la red del cliente B sede Pereira, realice las conexiones con la dirección 171.16.0.0/27. Registre las subredes en la siguiente tabla:

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| BSP-RS1 <>BSP-RBR | 0 | | |
| BSP-RS2 <>BSP-RBR | 1 | | |
| BSP-RG1 <>BSP-RBR | 2 | | |
| BSP-RG2 <>BSP-RBR | 3 | | |

## Cliente B sede Bogotá

El espacio de dirección para la red del cliente B sede Bogotá es el bloque de direcciones 11.2.0.0/16.

- BSB-RS1 necesita espacio para 32000 hosts
- BSB-RS2 necesita espacio para 16000 hosts

Divida el espacio de dirección para cada router de sucursal en tres subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| BSB-S1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |
| BSB-S2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

Para las WAN en la red del cliente B sede Bogotá realice las conexiones con la dirección 171.17.0.0/27. Registre las subredes en la siguiente tabla:

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| BSB-RG1 <>BSB-RG2 | 0 | | |
| BSB-RG1 <>BSB-RS1 | 1 | | |
| BSB-RG1 <>BSB-RS2 | 2 | | |
| BSB-RG2 <>BSB-RS1 | 3 | | |
| BSB-RG2 <>BSB-RS2 | 4 | | |

## Cliente C sede Cali

El espacio de direccionamiento para la red del cliente C sede Cali es el bloque de direcciones 12.1.0.0/19.

- CSC-RS1 necesita espacio para 4000 hosts
- CSC-RS2 necesita espacio para 2000 hosts _____

Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CSC-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| CSC-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

Para las WAN en la red del cliente C sede Cali realice las conexiones con la dirección 172.16.0.0/28. Registre las subredes en la siguiente tabla:

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CSC-RS1 <>CSC-RG | 0 | | |
| CSC-RS2 <>CSC-RG | 1 | | |
| CSC-RS1 <>CSC-RS2 | 2 | | |

## Cliente C sede Medellín

El espacio de direccionamiento para la red del cliente C sede Medellín es el bloque de direcciones 12.2.0.0/20.

- CSM-RS1 necesita espacio para 2000 hosts
- CSM-RS2 necesita espacio para 1000 hosts

Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CSM-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| CSM-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

Para las WAN en la red del cliente C sede Medellín realice las conexiones con la dirección 172.17.0.0/28. Registre las subredes en la siguiente tabla:

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| CSM-RS1 <>CSM-RBR | 0 | | |
| CSM-RS2 <>CSM-RBR | 1 | | |
| CSM-RG<>CSM-RBR | 2 | | |

## Cliente D sede Cali

El espacio de direccionamiento para la red del cliente D sede Cali es el bloque de direcciones 13.1.0.0/17.

- DSC-RS1 necesita espacio para 16 000 hosts _____
- DSC-RS2 necesita espacio para 8000 hosts
- DSC-RS3 necesita espacio para 8000 hosts _____

Divida el espacio de dirección para cada router de sucursal en tres subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| DSC-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |
| DSC-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |
| DSC-RS3 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| | e2/2 | 2 | | |

Para las WAN en la red del cliente D sede Cali realice las conexiones con la dirección 173.16.0.0/28. Registre las subredes en la siguiente tabla:

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| DSC-RS1 <>DSC-RG | 0 | | |
| DSC-RS2 <>DSC-RG | 1 | | |
| DSC-RS3 <>DSC-RG | 2 | | |

## Cliente D sede Medellín

El espacio de direccionamiento para la red del cliente D sede Medellín es el bloque de direcciones 13.2.0.0/18.

- DSM-RS1 necesita espacio para 8000 hosts __
- DSM-RS2 necesita espacio para 4000 hosts _
- DSM-RS3 necesita espacio para 4000 hosts

Divida el espacio de dirección para cada router de sucursal en dos subredes iguales. Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| DSM-RS1 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

| | | | | |
|---|---|---|---|---|
| DSM-RS2 | e2/0 | 0 | | |
| | e2/1 | 1 | | |
| DSM-RS3 | e2/0 | 0 | | |
| | e2/1 | 1 | | |

Para las WAN en la red del cliente B sede Medellín realice las conexiones con la dirección 173.17.0.0/27. Registre las subredes en la siguiente tabla:

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| DSM-RS1 <>DSM-RBR | 0 | | |
| DSM-RS2 <>DSM-RBR | 1 | | |
| DSM-RS3 <>DSM-RBR | 2 | | |
| DSM-RG <>DSM-RBR | 3 | | |

## Centro de Servicios VPN

El espacio de direccionamiento para la red del Centro de Servicios VPNes el bloque de direcciones 192.168.2.0/24.

- La LAN conectada a la interfaz e2/0 del router de CE (CS-VPN) e2/0 necesita 120 hosts
- La LAN conectada a la interfaz e2/1 del router de CE (CS-VPN) e2/1 necesita 55 hosts

Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| CS-VPN | e2/0 | 0 | | |
| | e2/1 | 1 | | |

## Red de administración VPN

El espacio de direccionamiento para la Red de administración VPNs el bloque de direcciones 192.168.3.0/24.

- La LAN conectada a la interfaz e2/0 del router de CE (RAD-VPN) e2/0 necesita 120 hosts
- La LAN conectada a la interfaz e2/1 del router de CE (RAD-VPN) e2/1 necesita 55 hosts Registre las subredes en la siguiente tabla:

| Router | Interfaz | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|---|
| RAD-VPN | e2/0 | 0 | | |
| | e2/1 | 1 | | |

## Red MPLS VPN

Para las WAN y las interfaces Loopback 0 en la red MPLS VPN realice las conexiones con la dirección 192.168.1.0/26. Registre las subredes en la siguiente tabla:

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| BOG-PE1<> P1 | 0 | | |
| BOG-PE1 <> P2 | 1 | | |
| CAL-PE2<> P1 | 2 | | |
| CAL-PE2 <> P2 | 3 | | |
| MED-PE3<> P3 | 4 | | |
| MED-PE3 <> P4 | 5 | | |
| PER-PE4<> P3 | 6 | | |
| PER-PE4 <> P4 | 7 | | |
| P1<> P2 | 8 | | |
| P1 <> P3 | 9 | | |
| P2<> P4 | 10 | | |
| P3 <> P4 | 11 | | |

Para las WAN que conectan las sedes de los clientes A, B, C y D a la red MPLS VPN, utilice la subred en la dirección 192.168.0.0/26.

| Conexión | Número de subred | Dirección de subred | Máscara de subred |
|---|---|---|---|
| ASB-RG1<>BOG-PE1 | 0 | | |
| ASB-RG2<>BOG-PE1 | 1 | | |
| BSB–RG1<>BOG-PE1 | 2 | | |
| BSB–RG2<>BOG-PE1 | 3 | | |
| CSC-RG <>CAL-PE2 | 4 | | |

| | | | |
|---|---|---|---|
| DSC-RG<>CAL-PE2 | 5 | | |
| CSM-RG<>MED-PE3 | 6 | | |
| DSM-RG<>MED-PE3 | 8 | | |
| ASP-RG<>PER-PE4 | 9 | | |
| BSP-RG1<>PER-PE4 | 10 | | |
| BSP-RG2 <>PER-PE4 | 11 | | |
| CS-VPN<>BOG-PE1 | 12 | | |
| RAD-VPN<>MED-PE3 | 13 | | |

**Paso 2:** Documente el esquema de direccionamiento.

- Documente las direcciones IP y máscaras de subred. Para los routers de sucursal asigne la primera dirección IP a la interfaz del router.
- En los enlaces WAN entre el cliente A, B, C y D y el domino MPLS utilice la primera dirección IP para los routers PE de la red MPLS VPN.

## TAREA 2: Aplicar una configuración básica.

**Paso 1:** Conecte una red que sea similar a la del diagrama de topología.

Utilizando GNS3 o equipos reales, conecte la topología que se muestra en el gráfico.

**Paso 2:** Configuración básica de los enrutadores

Realizar las configuraciones básicas de los enrutadores de acuerdo con las siguientes pautas generales (utilice como contraseña la palabra *"nyquist"*):

1. Configure el nombre de host del router.
2. Configure una contraseña de modo EXEC privilegiado.
3. Configure un mensaje del día.
4. Configure una contraseña para las conexiones de la consola.
5. Configure una contraseña para las conexiones de VTY.

## TAREA 3: Configurar el enrutamiento dinámico tanto en las sedes de los clientes A, B, C y D como en la red MPLS VPN.

**Paso 1:** Configurar el enrutamiento OSPF en el backbone MPLS VPN.

Configure el enrutamiento OSPF en los routers P Y PE de la red MPLS VPN. En la configuración, asegúrese de:

- Utilizar como identificador de proceso el número 1.
- Utilizar el área 0.

**Paso 2:** Configurar el enrutamiento RIPv2 en las sedes del cliente A.

Configure todos los routers en la redes de ambas sedes del cliente A con RIPv2 como protocolo de enrutamiento dinámico. En la configuración, asegúrese de:

- Deshabilitar la sumarización automática.
- Deshabilitar las actualizaciones RIP en las interfaces apropiadas.

**Paso 3:** Configurar el enrutamiento EIGRP en las sedes del cliente B.

Configure todos los dispositivos con un enrutamiento EIGRP en la redes de las sedes del cliente B. En la configuración, asegúrese de:

- Utilizar 100 como process-ID
- Desactivar la sumarización automática.

**Paso 4:** Configurar el enrutamiento OSPF en las sedes del cliente C.
Configure todos los dispositivos con un enrutamiento OSPF en la redes de las sedes del cliente C. En la configuración, asegúrese de:

- Utilizar 2 como process-ID.
- Utilizar el área 1.

**Paso 5:** Configurar el enrutamiento EIGRP en las sedes del cliente D.

Configure todos los dispositivos con un enrutamiento EIGRP en la redes de las sedes del cliente D. En la configuración, asegúrese de:

- Utilizar 200 como process-ID.
- Desactivar la sumarización automática.

## TAREA 4: Configurar MPLS modo trama en el backbone MPLS VPN

Paso 1: Habilitar la conmutación CEF.

Habilite la conmutación CEF en cada uno de los routers P y PE de la red MPLS VPN

Nota: El mecanismo de conmutación CEF está habilitado por defecto en las plataformas cisco 7100, 7200, 7500, 6500 y 12000.

**Paso 2:** Configurar MPLS modo trama en una interfaz.

En cada uno de los routers P y PE de la red MPLS VPN, habilite para cada router la conmutación de etiquetas en las interfaces adecuadas.

Paso 3: Configurar el MPLS ID en cada router.

Especifique la interfaz preferida para determinar el router ID LDP. Asegúrese que cada router en la red MPLS utilice la dirección de su interface Loopback 0 como identificador.

## TAREA 5: Configurar tablas VRF en los routers PE respectivos.

Para llevar a cabo el proceso de configuración de una tabla VRF e iniciar el despliegue de un servicio MPLS VPN para un cliente en necesario llevar seguir los siguientes pasos:

- Crear una tabla VRF
- Asignar un RD único a la VRF
- Asignar los import-exportRTs
- Asignar interfaces PE-CE a la VRF

Lleve a cabo el proceso de configuración de tablas VRFs para cada uno de los clientes que se conectan al backbone MPLS de acuerdo a las especificaciones planteadas en las siguientes tablas:

| Cliente | Router PE | VRF | RD | Imp RT | Exp RT | Int PE-CE | |
|---|---|---|---|---|---|---|---|
| A | BOG-PE1 | Cliente-RIP-ASB | 100:100 | 100:100 | 100:100 | S1/2 | S1/3 |
| | PER-PE4 | Cliente-RIP-ASP | 100:100 | 100:100 | 100:100 | S1/2 | |
| B | BOG-PE1 | Cliente-EIGRP-BSB | 100:110 | 100:110 | 100:110 | S1/4 | S1/5 |
| | PER-PE4 | Cliente-EIGRP-BSP | 100:110 | 100:110 | 100:110 | S1/3 | S1/4 |
| C | CAL-PE2 | Cliente-OSPF-CSC | 100:120 | 100:120 | 100:120 | S1/2 | |
| | MED-PE3 | Cliente-OSPF-CSM | 100:120 | 100:120 | 100:120 | S1/4 | |
| D | CAL-PE2 | Cliente-BGP-DSC | 100:130 | 100:130 | 100:130 | S1/3 | |
| | MED-PE3 | Cliente-BGP-DSM | 100:130 | 100:130 | 100:130 | S1/3 | |
| CEN-SER-VPN | BOG-PE1 | Central-Service | 100:200 | 100:200 | 100:200 | S1/6 | |
| RED-ADM-VPN | MED-PE3 | NMS-VPN | 100:140 | 100:140 | 100:140 | S1/2 | |

Tabla 4.12 Tabla de VRFs

## TAREA 6: Configurar sesiones MP-BGP entre los routers PE del backbone MPLS VPN

Para llevar a cabo esta tarea ejecute los siguientes pasos en cada router PE del backbone MPLS VPN:

- Defina 100 como número de sistema autónomo del proceso BGP.
- Defina la interfaz Loopback0 que servirá como BGP next-hop para las rutas VPNv4 y como dirección de origen para la sesión IBGP.
- Configure los routers PE remotos como vecinos bajo la configuración de enrutamiento BGP global.
- Especifique la dirección de origen para la sesiones MP-IBGP asegurándose de que dichas sesiones sean ejecutadas entre las interfaces Loopback 0 definidas para cada router PE.
- Seleccione la familia de direcciones VPNv4.
- Active los routers PE remotos para el intercambio de ruta VPNv4.
- Garantice que la interfaz Loopback 0 será siempre la dirección de siguiente salto BGP para las rutas VPNv4 que serán propagadas por este router a sus vecinos MP-IBGP.
- Configure la propagación de los atributos community estándar y extendido.

## TAREA 7: Conectar las sedes del cliente A a través del backbone MPLS VPN

**Paso 1:** Establezca sesiones de enrutamiento RIP PE-CE entre los routers CE de ambas sedes y los routers PE respectivos.

Para cada router PE asociado a este Cliente:

- Configure el proceso de enrutamiento RIP global. Asegúrese de establecer el número de versión (Versión 2) como parámetro global y deshabilite la sumarización automática.
- Cree un contexto de enrutamiento RIP asociándolo con la instancia VRF respectiva. Lleve a cabo esta operación con base en las especificaciones establecidas en la tabla de VRFs.
- Habilite la o las interfaces PE-CE en el contexto de enrutamiento RIP de modo que se lleve a cabo el intercambio de actualizaciones RIPv2 con los routers CE respectivos.

**Paso 2:** Establezca la conectividad RIPv2 de extremo a extremo

Para cada router PE asociado a este Cliente:

- Cree una instancia del proceso global BGP, asócielo con la tabla VRF relacionada con este cliente y posteriormente redistribuya las rutas RIPv2 vinculadas a dicha tabla de

enrutamiento virtual. Lleve a cabo esta operación con base en las especificaciones establecidas en la tabla de VRFs.
- Desde las instancias del proceso RIP creada previamente en cada router PE redistribuya las rutas BGP pertenecientes a las tablas VRF relacionadas con este cliente.

## TAREA 8: Conectar las sedes del cliente B a través del backbone MPLS VPN

**Paso 1:** Establezca sesiones de enrutamiento EIGRP PE-CE entre los routers CE de ambas sedes y los routers PE respectivos.

Para cada router PE asociado a este Cliente:

- Configure el proceso de enrutamiento EIGRP global utilizando 1 como identificador de proceso. Deshabilite la sumarización automática.
- Configure el contexto de enrutamiento EIGRP del proceso EIGRP global asociándolo con la instancia VRF respectiva y posteriormente especifique el número de identificador de proceso EIGRP (process-id 100) que ejecutan los routers CE vinculados a este cliente de modo que se establezcan adyacencias con dichos routers. Lleve a cabo esta operación con base en las especificaciones establecidas en la tabla de VRFs.
- Habilite la o las interfaces PE-CE en el contexto de enrutamiento EIGRP de modo que se lleve a cabo el intercambio de actualizaciones EIGRP con los routers CE respectivos.

**Paso 2:** Establezca la conectividad EIGRP de extremo a extremo Para cada router PE asociado a este Cliente

- Cree una nueva instancia del proceso global BGP, asócielo con la tabla VRF adecuada y posteriormente redistribuya las rutas EIGRP vinculadas a este cliente haciendo referencia al número de proceso EIGRP que se ejecutan en c/u de sus sedes. Lleve a cabo esta operación con base en las especificaciones establecidas en la tabla de VRFs.
- Desde la instancia del proceso EIGRP creada previamente redistribuya las rutas BGP pertenecientes a las tablas VRF relacionadas con este cliente.

## TAREA 9: Conectar las sedes del cliente C a través del backbone MPLS VPN

**Paso 1:** Establezca sesiones de enrutamiento OSPF PE-CE entre los routers CE de ambas sedes y los routers PE a los que están conectados

Para cada router PE asociado a este cliente:

- Configure un nuevo proceso de enrutamiento OSPF independiente, diferente al proceso OSPF utilizado como IGP para la red MPLS y asócielo con la instancia VRF vinculada a este cliente. Lleve a cabo esta operación con base en las especificaciones establecidas en la tabla de VRFs. (Por uniformidad establezca como identificador de proceso OSPF el mismo process-id definido en los procesos OSPF configurados por este cliente en los routers de cada una de sus sedes).
- Habilite la interfaz PE-CE en el proceso de enrutamiento OSPF a través del comando network asegurándose de que el parámetro área sea el mismo que se definido en los procesos OSPF configurados por el cliente (área 1) de modo que se lleve a cabo el intercambio de actualizaciones con el routers CE respectivos.

**Paso 2:** Establezca la conectividad OSPF de extremo a extremo Para cada router PE asociado a este Cliente:

- Cree una nueva instancia del proceso global BGP y asócielo con la tabla VRF adecuada, y desde allí redistribuya las rutas OSPF vinculadas a este cliente. Lleve a cabo esta operación con base en las especificaciones establecidas en la tabla de VRFs.
- Desde el proceso OSPF creado previamente redistribuya las rutas MP-BGP pertenecientes a las tablas VRF relacionadas con este cliente.

## TAREA 10: Conectar las sedes del cliente D a través del backbone MPLS VPN

**Nota:** Utilice 65501 como identificador de proceso para los procesos BGP ejecutados en las sedes de este cliente.

**Paso 1:** Establezca mallas completas de sesiones BGP en las sedes de este cliente.

**Paso 1.1:** Establezca una malla completa de sesiones IBGP en la sede Cali.

- Desde el router CE DSC-RG establezca sesiones IBGP a los demás routers C.
- Desde los routers C establezca sesiones IBGP con el router CE.

**Paso 1.2:** Establezca una malla completa de sesiones IBGP en la sede Medellín.

- Desde el router CE DSM-RG establezca sesiones IBGP a los demás routers C.
- Desde los routers C establezca sesiones IBGP con el router CE.

**Paso 2:** Establezca la conectividad BGP de extremo a extremo Para cada router CE asociado al Cliente D:

- Desde el proceso de enrutamiento BGP redistribuya las rutas del proceso EIGRP ejecutado en las sedes este cliente.
- Establezca la relación de vecinos EBGP entre cada router CE y el router PE al que se conecta.

Para cada router PE asociado al Cliente D:

- Cree una nueva instancia del proceso global BGP y asócielo con la tabla VRF adecuada. Lleve a cabo esta operación con base en las especificaciones establecidas en la tabla de VRFs.
- Desde esta nueva instancia de enrutamiento BGP establezca la relación de vecinos EBGP con los routers CE respectivos tal como lo muestra el diagrama de topología.
- Asegúrese que las actualizaciones de enrutamiento BGP entre ambas sedes de este cliente no sean bloqueadas entre sí.

## TAREA 11: Conectar la red del Centro de Servicios VPN al backbone MPLS VPN

**Nota:** Utilice 65502 como identificador de proceso para los procesos BGP ejecutado en la red del Centro de Servicios VPN.

**Paso 1:** Publique las redes del Centro de Servicios VPN.

Anuncie la red 192.168.2.0/24 desde el router PE de la red del Centro de Servicios VPN mediante el comando **network.**

**Paso 2:** Establezca la conectividad BGP entre la red del Centro de Servicios VPN y la red MPLS

- 
- En el router PE vinculado al Centro de Servicios VPN cree una nueva instancia del proceso global BGP y asócielo con la tabla VRF adecuada. Lleve a cabo esta operación con base en las especificaciones establecidas en la tabla de VRFs.
- Desde esta nueva instancia de enrutamiento BGP establezca la relación de vecinos EBGP con el router CE del Centro de Servicios VPN tal como lo muestra el diagrama de topología.
- Desde el proceso de enrutamiento BGP que ejecuta el router CE del Centro de Servicios establezca la relación de vecinos EBGP con el routerPE respectivo.

## TAREA 12: Conectar la Red de Administración VPN al backbone MPLS VPN

**Nota:** Utilice 65503 como identificador de proceso para el proceso BGP ejecutado en la Red de Administración VPN.

**Paso 1:** Publique las redes de la Red de Administración VPN.

Anuncie la red 192.168.3.0/24 desde el router PE de la Red de Administración VPN mediante el comando **network.**

**Paso 2:** Establezca la conectividad BGP entre la Red de Administración VPN y la red MPLS VPN.

- En el router PE vinculado a la Red de Administración VPN cree una nueva instancia del proceso global BGP y asócielo con la tabla VRF adecuada. Lleve a cabo esta operación con base en las especificaciones establecidas en la tabla de VRFs.
- Desde esta nueva instancia de enrutamiento BGP establezca la relación de vecinos EBGP con el router CE de la Red de Administración VPN tal como lo muestra el diagrama de topología.
- Desde el proceso de enrutamiento BGP que ejecuta el router CE de la Red de Administración VPN establezca la relación de vecinos EBGP con el routerPE respectivo.

## TAREA 13: Conectar las oficinas centrales de los clientes A y D mediante la solución Overlapping VPN.

Cuando dos clientes desean compartir información, podrían decidir interconectar sus sitios centrales. Para lograr esto, se deben crear dos VPN simples que contendrán el sitio central y los sitios remotos del cliente respectivo. A continuación se debe crear una VPN adicional que se superpone parcialmente con las VPNs de ambos clientes y conectará sus sitios centrales. De este modo los sitios centrales de ambos clientes podrán comunicarse entre sí. Los sitios centrales podrán comunicarse además con los sitios remotos pertenecientes a su propia VPN, pero no con los sitios remotos pertenecientes a la VPN simple asociada con el otro cliente. A esta solución se le denomina **Overlapping VPN**.[48]

Como muestra la topología tanto el cliente A como el cliente D tienen dos sedes a nivel nacional que se interconectan a través de la red MPLS VPN de un proveedor de servicio de internet. El cliente A tiene su sede central en la ciudad de Bogotá y cuenta además con una sucursal en la ciudad de Pereira. El cliente D a su vez opera en las ciudades de Cali y Medellín siendo esta última la sede de su oficina principal. La conexión de las sedes de ambos clientes a través del dominio MPLS VPN se realiza mediante el establecimiento de VPNs simples.

El objetivo de este ejercicio es conectar las sedes principales de ambos clientes asegurándose que las sedes restantes no puedan comunicarse entre sí. En otras palabras configure la red MPLS VPN de tal forma que las redes anunciadas por la sede Bogotá del cliente A puedan alcanzar las redes anunciadas por la sede Medellín del cliente D garantizando que la sede

Bogotá del cliente A no pueda alcanzar los prefijos anunciados por la sede Cali del cliente D y que la sede central del cliente D ubicada en Medellín no pueda alcanzar los prefijos anunciados por la sede Pereira del cliente A.

A continuación se muestra una tabla que responde a los requisitos configuración de overlapping VPN que se utilizará para dar solución al desafío previamente planteado. Note que esta tabla tiene unos campos RT en blanco.

48 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p.200

Llénelos de acuerdo a los requerimientos de conexión planteados y establezca las configuraciones respectivas.

| VRF | RD | Imp RT | | Exp RT | |
|---|---|---|---|---|---|
| Cliente-RIP-ASB | 100:101 | 100:100 | 100:500 | 100:100 | 100:500 |
| Cliente-RIP-ASP | 100:100 | 100:100 | | 100:100 | |
| Cliente-BGP-DSC | 100:130 | 100:130 | | 100:130 | |
| Cliente-BGP-DSM | 100:131 | 100:130 | 100:500 | 100:130 | 100:500 |

Investigue cuales son los usos típicos de las solución *Overlapping VPN*

---

## TAREA 14: Conectar las sedes de los clientes B y C a un conjunto de servidores común mediante la solución *Central Services VPN*

Un centro de servicios VPN (*central services VPN*) se utiliza cuando un grupo de VPNs comparte un conjunto común de servidores. Este conjunto de servidores se ubica al interior del centro de servicios VPN y todas las demás VPNs tienen acceso a ellos. Sin embargo, las VPNs asociadas al centro de servicios no pueden comunicarse entre sí. Para implementar esta solución el centro de servicios VPN utiliza dos valores RT (*route-target*), uno para importar redes desde los clientes respectivos en la VPN y otro para exportar las redes de origen local hacia dichos clientes. Los clientes por su parte hacen lo opuesto utilizando un RT para importar las redes del centro de servicios VPN y otro RT adicional para exportar sus redes de origen local hacia el centro de servicios.[65]

65 Cisco Systems Learning. Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p.209.

Como muestra la topología tanto el cliente B como el cliente C tienen dos sedes a nivel nacional que se interconectan a través de la red MPLS VPN de un proveedor de servicio de internet. La conexión de las sedes de ambos clientes a través del dominio MPLS VPN se realiza mediante el establecimiento de VPNs simples.

Ambos clientes han decidido utilizar el centro de servicios VPN que ofrece el ISP de manera que ambos puedan centralizar su información corporativa y a su vez compartirla. Para lograr esto debe asegurarse que exista una conexión bidireccional entre el centro de servicios VPN y las VPN de cada cliente. Debe asegurarse además que no exista comunicación entre las VPNs de ambos clientes.

A continuación se muestra un esquema de numeración RD-RT que responde a los requisitos de configuración de la solución *central services VPN* que se utilizará para resolver al desafío previamente planteado. Note que esta tabla tiene unos campos RT en blanco. Llénelos de acuerdo a los requerimientos de conexión planteados y establezca las configuraciones respectivas.

| VRF | RD | Imp RT | | Exp RT | |
|---|---|---|---|---|---|
| Cliente-EIGRP-BSB | 100:110 | 100:110 | 100:600 | 100:110 | 100:601 |
| Cliente-EIGRP-BSP | 100:110 | 100:110 | 100:600 | 100:110 | 100:601 |
| Cliente-OSPF-CSC | 100:120 | 100:120 | 100:600 | 100:120 | 100:601 |
| Cliente-OSPF-CSM | 100:120 | 100:120 | 100:600 | 100:120 | 100:601 |
| Central-Service | 100:200 | 100:200 | 100:601 | 100:200 | 100:600 |

Investigue cuales son las situaciones típicas en la que necesario el uso de esta topología

_____
_____
_____

## TAREA 15: Conectar las sedes centrales de los clientes B y C a un conjunto de servidores común

En la actividad anterior se llevó a cabo una configuración en la que las sedes de los clientes A y B se conectaron a un centro de servicios VPN con el objetivo de centralizar y compartir su información corporativa. El objetivo de esta actividad es modificar la tarea anterior de manera que solo las oficinas centrales de ambos clientes tengan acceso a los servidores centrales ubicados en el centro de servicios VPN mientras que las demás sedes de cada cliente tengan acceso solo a los sitios pertenecientes a su propia VPN.

Modifique el esquema de numeración RD-RT anterior de manera que cumpla con los nuevos requisitos de conectividad y establezca las configuraciones respectivas.

¿Es necesario modificar los valores RD de las VRF asociadas a las oficinas centrales de cada cliente?

¿Por qué?

_____
_____
_____
_____

## TAREA 16: Implementar la solución Managed CE RoutersService para administrar los routers CE de los clientes

Un proveedor de servicio puede implementar una red de administración VPN independiente para gestionar los routers CE de todas las VPNs asociadas a los clientes que se conectan al backbone MPLS VPN. Esta red de administración VPN debe tener acceso a todos los routers CE de cada cliente pero no debe tener acceso a los demás sitios pertenecientes a las instalaciones del mismo. Pala lograr este objetivo es necesario el uso de un par de valores RT. Un RT se utiliza para exportar las direcciones loopback de los routers CE e importar dichas direcciones en la VRF de la red de administración VPN. El RT restante es utilizado para exportar las redes de la VRF asociada con la red de administración VPN e importar estas redes en todas las demás VRFs.[66]

Señales las semejanzas y diferencias entre este diseño y la implementación de un centro de servicios VPN

_____
_____
_____
_____

El proveedor de servicio ha implementado una red de administración VPN y a través de esta red gestionará los routers CE de todos los clientes conectados al backbone MPLS VPN.

| VRF | RD | Imp RT | Exp RT |
|---|---|---|---|
| Cliente-RIP-ASB | 100:100 | | |
| Cliente-RIP-ASP | 100:100 | | |
| Cliente-EIGRP-BSB | 100:110 | 100:110 | 100:110 |
| Cliente-EIGRP-BSP | 100:110 | 100:110 | 100:110 |
| Cliente-OSPF-CSC | 100:120 | 100:120 | 100:120 |

66 Cisco Systems Learning.Implementing Cisco MPLS. Volume 1. Version 2.1. Estados Unidos. 2004. p.226.

| | | | | |
|---|---|---|---|---|
| Cliente-OSPF-CSM | 100:120 | 100:120 | | 100:120 |
| Cliente-BGP-DSC | 100:130 | | | |
| Cliente-BGP-DSM | 100:130 | | | |
| NMS-VPN | 100:140 | | | |

Complete esta tabla con los RTs faltantes de acuerdo a las especificaciones antes mencionadas y establezca las configuraciones pertinentes.

Para llevar a cabo esta actividad es necesario marcar las direcciones *Loopback* los routers CE de cada cliente de manera que solo estas direcciones sean importadas en tabla VRF (NMS-VPN) asociada a la red de administración VPN.

Utilice los siguientes comandos para llevar a cabo esta tarea de forma exitosa.

- Importmaproute-map-name modo de configuración vrf.
- Exportmaproute-map-name modo de configuración vrf.
- route-mapnamepermitseq modo de configuración global.
  matchcondition
  set excommunity rt value [additive]

**NOTA:** La tabla anterior no contempla los cambios en los valores RT-RD necesarios para implementar las tareas anteriores.

En este libro se encontrará un complemento a los libros de contenidos teóricos generados a través del Proyecto de Innovación "Plataforma de emulación de servicios sobre redes inteligentes" en el marco del proyecto desarrollado por la Universidad Tecnológica de Pereira para la conformación del Centro de Innovación y Desarrollo Tecnológico, alrededor de las temáticas relacionadas con los protocolos de comunicación BGP – Border Gateway Protocol y MPLS Multiprotocol Label Switching.

Se presentan una serie de laboratorios prácticos que permiten que los profesionales del área de las telecomunicaciones y carreras afines profundicen y afiancen conceptos de BGP, desde sus características, tipos de usuarios, atributos, conectividad, escalabilidad y optimización. Así como conceptos básicos y esenciales del protocolo MPLS, ingeniería de tráfico, arquitectura de una red MPLS y funcionamiento de las etiquetas desde su asignación, distribución y hasta su implementación en redes virtuales privadas VPN. Permitiendo conseguir la apropiación de dichos conocimientos. Estos laboratorios propuestos se presentan como una estrategia de enseñanza para la comprensión de los conceptos teóricos.

Cada una de las prácticas ha sido planeada y estructurada con base en los recursos disponibles en el laboratorio a través de la plataforma de emulación de servicios desplegada y con base en los contenidos específicos que permiten diseñar y mantener redes de transporte a nivel de conmutación y enrutamiento.

**ISBN: 778-958-722-315-6**

**Universidad Tecnológica de Pereira**